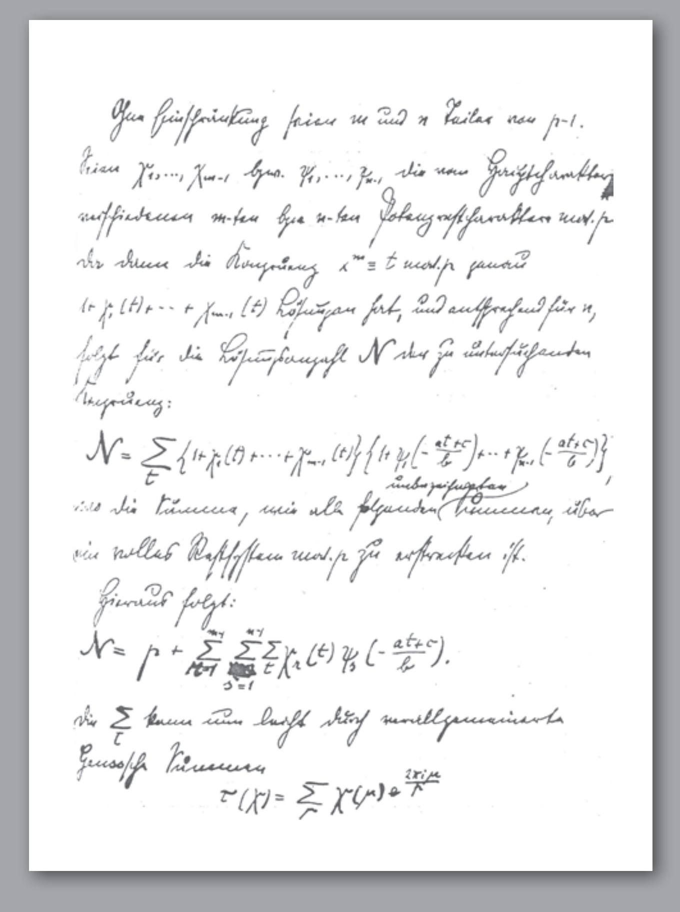
Die mathematischen Tagebücher von Helmut Hasse 1923 – 1935

Herausgegeben und kommentiert von
Franz Lemmermeyer und Peter Roquette

With an Introduction in English



Zur Einschränkung seien m und n Teiler von $p-1$. Seien $\chi_1, \ldots, \chi_{m-1}$ bzw. $\psi_1, \ldots, \psi_{n-1}$ die vom Hauptcharakter verschiedenen m-ten bzw. n-ten Potenzrestcharaktere mod. p. Da dann die Kongruenz $x^m \equiv t$ mod. p genau $1+\chi_1(t)+\cdots+\chi_{m-1}(t)$ Lösungen hat, und entsprechend für n, folgt für die Lösungsanzahl N der zu untersuchenden Kongruenz:

$$N = \sum_t \{1+\chi_1(t)+\cdots+\chi_{m-1}(t)\}\{1+\psi_1(-\tfrac{at+c}{b})+\cdots+\psi_{n-1}(-\tfrac{at+c}{b})\},$$

wo die Summe, wie alle folgenden unbezeichneten Summen, über ein volles Restsystem mod. p zu erstrecken ist.

Hieraus folgt:

$$N = p + \sum_{r=1}^{m-1}\sum_{s=1}^{n-1}\sum_t \chi_r(t)\,\psi_s(-\tfrac{at+c}{b}).$$

Die $\sum_t$ kann nun leicht durch verallgemeinerte Gaussche Summen

$$\tau(\chi) = \sum_\mu \chi(\mu)\, e^{\frac{2\pi i \mu}{p}}$$

Universitätsverlag Göttingen

Franz Lemmermeyer, Peter Roquette (Hg.)

Die mathematischen Tagebücher von Helmut Hasse 1923 - 1935

erschienen im Universitätsverlag Göttingen 2012

Franz Lemmermeyer und
Peter Roquette (Hg.)

Die mathematischen Tagebücher von Helmut Hasse 1923 - 1935

With an introduction in English



Universitätsverlag Göttingen
2012

Bibliographische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Kontakt / Contact
Peter Roquette
Universität Heidelberg
roquette@uni-hd.de

Franz Lemmermeyer
Gymnasium St. Gertrudis, Ellwangen
hb3@ix.urz.uni-heidelberg.de

Satz und Layout: Thomas Olschewski
Umschlaggestaltung: Jutta Pabst
Titelabbildung: Tagebuch VII, 1931-1935, S. 13
Quelle: Handschriftenabteilung der Niedersächsischen Staats- und Universitätsbibliothek Göttingen (Cod. Ms. H. Hasse 16 : 1)

http://univerlag.uni-goettingen.de
ISBN: 978-3-86395-072-9

Übersicht

Teil I

Vorspann

Introduction

This edition contains the text of the notebooks (*Tagebücher*) of Helmut Hasse (1898–1979). There are seven volumes with altogether 98 entries, spanning the time period from July 1923 to February 1935. We have preceded each entry with a short comment in English.

In the Dictionary of Scientific Biography we read:

> *Helmut Hasse, one of the most important mathematician of the twentieth century, was a man whose accomplishments spanned research, mathematical exposition, teaching and editorial work.*

In view of this it may be of interest to learn more about the work of Hasse, not only through his publications but also from their background.

In this respect the Hasse collection in the *Handschriftenabteilung* of Göttingen University Library is a treasure trove for historic research; it contains a large amount of letters, manuscripts and notes. We have already edited and commented two of the most noteworthy letter files in this collection: the letters Hasse–Emmy Noether [LR06] and the letters Hasse–Emil Artin [FR08]. More is planned to come. And here are his notebooks.

Whereas the mentioned letters admit a glance at the gradual evolvement of Hasse's mathematical ideas which later found their way into his publications, the notebooks are of a different kind. They open up a colorful kaleidoscope of various mathematical activities of Hasse, his mathematical background, his mathematical interests, and his way of approaching problems. Most of the entries are inspired by discussions with other mathematicians (quite often the name of Artin is mentioned), but sometimes he obtains his motivation from the literature.

We can find very brief entries like the definition of groups by generators and relations (3.1), or a technical result on the prime decomposition in subfields of

the decomposition field (3.17). We also find entries about problems which Hasse had heard from colleagues, like Knopp's or Ostrowski's questions (3.11) and (4.12). Some entries have almost the character of recreational math, like Kirkman's problem of 15 school girls (3.2), or construction with ruler and compass (4.14). We find text for use in class like the theory of the real Gamma function in (4.6) or Fermat's problem for the exponent five in (7.2.)

But there are also more serious entries on number theory which point towards later development in Hasse's research, like the one about Kummer's logarithmic derivatives (1.5.), or the first proof of the Riemann hypothesis for the Davenport-Hasse curves in (7.4.) And there are extended expositions like the one on the class number of abelian fields (1.9) or on the computation of units by continued fractions in quadratic fields (1.14), and by the Jacobi-Perron algorithm in cubic fields (2.2). We also find the entry of September 27, 1927 which is worldwide the first document where Artin's conjecture on primitive roots is mentioned (4.8).[1]

The reader who looks at the table of contents will discover more entries of interest.

The last four entries in Hasse's 7-th notebook are dated February 1934. However there is some discrepancy with respect to the dates, since the foregoing entries are dated for 1935. A possible explanation is that right after February 1934 Hasse was absorbed with the work on his project of proving the Riemann hypothesis for function fields, and thus he did not take proper care of his notebook.

Indeed, in the days from the 5th to 9th February, 1934 Hasse had visited Hamburg where he gave a series of lectures on his new proof of the Riemann hypothesis for elliptic curves. During this visit there were many occasions for extended discussions with Artin. In fact, all the above mentioned four last entries are marked with the name of Artin. But the most important topic of the discussions with Artin during these days is not mirrored in Hasse's note book: This was the way how to approach the Riemann hypothesis for curves of higher genus $g > 1$. In fact, Hasse reported to Davenport on February 12, 1934:

> *From what Artin and I found when considering the possibilities of generalisation to higher genus, it becomes only a matter of patience to do this. The general line is fully obvious now ...*

Well, it turned out that it required something more than patience to establish all the details necessary for the generalization to higher genus, even if the general

[1]More extended manuscripts containing original work of Hasse were not written into the notebooks and are not included here. It is planned to edit some of them in another volume.

line seemed "fully obvious" to Artin and Hasse. Therefore, Hasse first concentrated his work on a special class of curves of higher genus, namely those which today are called the "Davenport-Hasse curves". These papers were to appear in 1934.

So it seems that Hasse did not find the time to write down the said four entries immediately after his visit to Artin, in particular since these topics did not have immediate connection to his work on curves or function fields. And that it was one year later only that he again turned to his notebook and remembered his discussions with Artin in 1934.

We also have to take into account that the years 1933 and 1934 had brought extreme political troubles. The story about the opposition which Hasse had to face from his Nazi colleagues and students in Göttingen is well known and need not be repeated here. In any case it is understandable that during the summer semester 1934 he did not find much of the quiet atmosphere which seems necessary for mathematical thoughts. In consequence he did not update his notebook. In fact, on February 12, 1934 he wrote from Marburg to his friend Davenport about the "battle" which he would have to expect in Göttingen:

> *I very much hope that I shall have a quiet summer here before I am called upon the battle field. Otherwise I doubt whether I shall be able to think on $f(x, y) = 0$ for higher genus before long.*

We know that his wish for a quiet summer 1934 did not materialize. Much later we read in a letter of December 15, 1935 from Hasse to Siegel the following:[2]

> *Since May 1934 I had to interrupt thoroughly my scientific work, and it was last October only when I was able to take up my research again.*

But the notebook was not continued after 1935.

Heidelberg, March 2012

Peter Roquette
Franz Lemmermeyer

[2]Translation from German.

Acknowledgements:

This work was partially supported by the *Deutsche Forschungsgemeinschaft* and the *Möllgaard-Stiftung*. The transcription from the original into LaTeX was done by Dipl. math. Thomas Olschewski, including the preparation of the index and the bibliography.

Remarks:

1. Each notebook is preceded by a list of contents. In addition the reader will find a comprehensive list of contents immediately after the introduction.
2. Hasse's own footnotes are marked with symbols whereas our footnotes are marked with numbers.
3. The original page numbers in Hasse's notebooks are indicated by numbers on the margin. For instance, the number IV, 51 on the margin indicates the beginning of Hasse's page 51 in the fourth notebook.

Inhaltsverzeichnis

Teil II

Die Tagebücher

Kapitel 1

Tagebuch I: Juli 1923 – November 1923

Eintragungen

1.1 Gitter–Beweis des quadratischen Reziprozitätsgesetzes im rationalen Körper (Frobenius). (Mitteilung von Dr. Artin). (17.7.1923)

Frobenius published two proofs of the quadratic reciprocity law: a modification of Zeller's proof in [Fro14a]*, and a variant of Eisenstein's proof based on lattice points in* [Fro14b]*. The proof sketched here is Frobenius' second proof. Artin had visited Hasse in Kiel on the weekend July 14-16, 1923 in order to work with Hasse on their joint paper on the 2nd supplement of the reciprocity law for odd prime exponents* [AH25]*. We see that they also talked about the quadratic reciprocity law.*

I, 4

17. VII. 23.

1.) Gausssches Lemma:

d prim zu p, $\left(\frac{d}{p}\right) \equiv d^{\frac{p-1}{2}} \mod p$.
Behauptung: $\left(\frac{d}{p}\right) = (-1)$ hoch der Anzahl der absolut kleinsten, negativen Reste der $\frac{p-1}{2}$ Multipla $d, 2d, \ldots, \frac{p-1}{2}\, d$.
Beweis: s. Dirichlet–Dedekind, S. 96/97.

2.) Beweis des Reziprozitätsgesetzes:

p, q positive, ungerade Primzahlen, x durchlaufe alle Zahlen $1, 2, \ldots, \frac{p-1}{2}$. Dann entspricht jedem x *eindeutig* ein ganzes y, sodaß

$$-\frac{p}{2} < qx - py < +\frac{p}{2} \tag{1}$$

und es ist $\left(\frac{q}{p}\right) = (-1)$ hoch der Anzahl der Zahlen (1) im Intervall $-\frac{p}{2} \ldots 0$.

Es genügt in (1) das y auf die Werte $1, 2, \ldots, \frac{q-1}{2}$ zu beschränken. Denn aus (1) folgt einerseits

$$\begin{array}{lcl} & y & < \frac{q}{p}x + \frac{1}{2} < \frac{q}{2} + \frac{1}{2} = \frac{q+1}{2}\,, \\ \text{also} & y & \leqq \frac{q-1}{2} \\ \text{Andererseits} & y & > \frac{q}{p}x - \frac{1}{2} > -\frac{1}{2}\,, \\ \text{also} & y & \geqq 0\,. \end{array}$$

Da aber $y = 0$ stets zu einem $qx - py > 0$ führt, kommt dieser Wert nicht in Frage. Also ist

$$\left(\frac{q}{p}\right) = (-1) \text{ hoch der Anzahl der Zahlen } qx-py \text{ zwischen } -\tfrac{p}{2} \text{ und } 0\text{, wenn } \left\{\begin{matrix} 1 & \leqq & x & \leqq & \frac{p-1}{2} \\ 1 & \leqq & y & \leqq & \frac{q-1}{2} \end{matrix}\right\}.$$

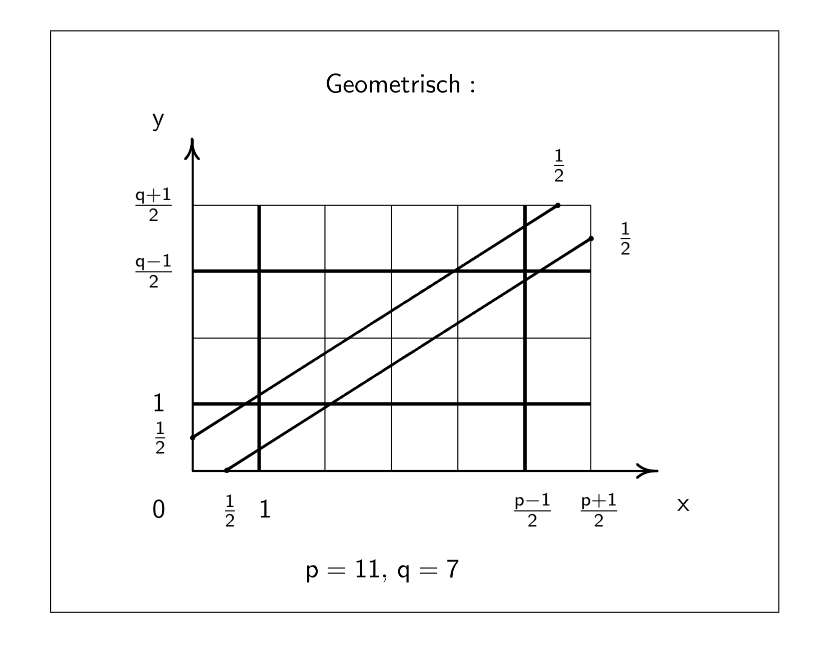
I, 5 Ebenso:

$$\left(\frac{p}{q}\right) = (-1) \text{ hoch der Anzahl der Zahlen } py-qx \text{ zwischen } -\tfrac{q}{2} \text{ und } 0\text{, wenn } x, y \text{ in denselben Grenzen}$$

$$\text{oder auch } = (-1) \text{ hoch der Anzahl der Zahlen } qx - py \text{ zwischen } 0 \text{ und } \tfrac{q}{2}\,.$$

Also:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1) \text{ hoch der Anzahl der Zahlen } -\tfrac{p}{2} < qx-py < +\tfrac{q}{2}\,, \text{ wenn } \left\{\begin{matrix} x = 1, 2, \ldots \frac{p-1}{2} \\ y = 1, 2, \ldots \frac{q-1}{2} \end{matrix}\right\}.$$



Es ergibt sich Symmetrie des Streifens zwischen den beiden Parallelen

$$\begin{aligned} qx - py &= -\frac{p}{2} \\ qx - py &= +\frac{q}{2} \end{aligned}$$

dessen Gitterpunkte abzuzählen sind, bezüglich des Rechteckes

x	1	$\frac{p-1}{2}$
y	1	$\frac{q-1}{2}$

Denn die „Eckabstände " ergeben sich zu $\frac{1}{2}$. Also darf [...] die Anzahl der Gitterpunkte dieses ganzen Rechteckes genommen werden d. h.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$$

Arithmetisch: Ist: I, 6

$$qx - py > \frac{q}{2}$$

so folgt für den „spiegelbildlichen Gitterpunkt" $\left\{ \begin{array}{l} \frac{p+1}{2} - x = x' \\ \frac{q+1}{2} - y = y' \end{array} \right\}$:

$$\begin{aligned} qx' - py' &= -qx + py + q\,\frac{p+1}{2} - p\,\frac{q+1}{2} \\ &= -(qx - py) + \frac{q}{2} - \frac{p}{2} > -\frac{p}{2} \end{aligned}$$

also

$$qx' - py' < -\frac{p}{2}$$

Jedem Gitterpunkt, der nach der einen Seite aus dem Intervall herausfällt, entspricht also ein spiegelbildlicher, der es nach der anderen Seite tut. Diese dürfen also, da sie *paarweise* auftreten, mitgerechnet werden, also kann die Anzahl *aller* Gitterpunkte genommen werden, was wieder

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$$

ergibt.

1.2 Eulersche Summenformel, Stirlingsche Reihe. (17.7.1923)

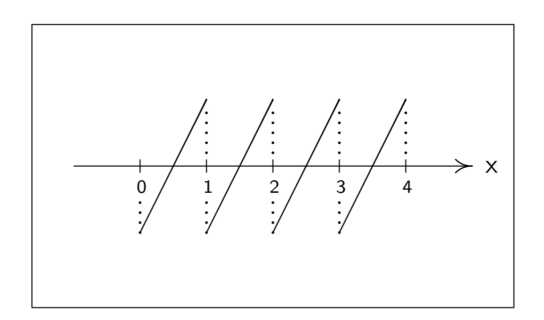
The Euler-MacLaurin summation formula is a fundamental tool in analytic number theory. For a detailed account of the early history of this formula, see Schuppener [Sch94]*. Here, Hasse derives the summation formulas of Euler and Dirichlet, and applies this to derive the functional equation of the theta function. This entry is another fruit of Artin's visit to Hasse in Kiel.*

I, 7

(Nach Dr. Artin, 17. VII. 23).

Wir betrachten die unstetige Funktion, periodisch in x mit der Periode 1:

$$\psi(x) = x - [x] - \frac{1}{2}$$



$f(x)$ sei eine volle, beliebig oft stetig differenzierbare Funktion. Wir bilden

$$\int\limits_0^n \psi(x) f'(x)\,dx = \int\limits_0^n x f'(x)\,dx - \frac{1}{2}\int\limits_0^n f'(x)\,dx - \int\limits_0^n [x] f'(x)\,dx$$

$$= -\int\limits_0^n f(x)\,dx + nf(n) - \frac{1}{2}\big(f(n) - f(0)\big) - \sum_{\nu=0}^{n-1} \nu \int\limits_\nu^{\nu+1} f'(x)\,dx$$

das letzte Glied ist

$$\sum_{\nu=0}^{n-1} = \sum_{\nu=0}^{n-1} \nu \big(f(\nu+1) - f(\nu)\big) = \sum_{\nu=1}^{n} (\nu-1) f(\nu) - \sum_{\nu=0}^{n-1} \nu f(\nu) = -\sum_{\nu=1}^{n} f(\nu) + n\, f(n)\,,$$

also

$$\int_0^n \psi(x) f'(x)\, dx = -\int_0^n f(x) dx - \frac{1}{2}\big(f(n) + f(0)\big) + \sum_{\nu=0}^{n} f(\nu)$$

$$\boxed{\sum_{\nu=0}^{n} f(\nu) = \int_0^n f(x)\, dx + \frac{1}{2}\Big[f(n) + f(0)\Big] + \int_0^n \psi(x) f'(x)\, dx}$$

Diese Formel ist als der eigentliche Kern der Eulerschen Summenformel anzusehen.

Um sie weiter zu verwerten ist das Restintegral durch partielle Integration auszuwerten, oder wenigstens durch Näherungsglieder zu approximieren. I, 8

Dazu entwickelt man $\psi(x)$ in eine Fourier–Reihe. $\psi(x)$ ist periodisch mit der Periode 1. Also sind die Fourier–Koeffizienten von

$$\psi(x) = \sum_{-\infty}^{+\infty} c_\nu\, e^{2\pi i \nu x} \qquad \text{für } \nu \neq 0:$$

$$\begin{aligned}
c_\nu &= \int_0^1 \psi(x)\, e^{-2\pi i\nu x}\, dx = \int_0^1 \left(x - \frac{1}{2}\right) e^{-2\pi i\nu x}\, dx \\
&= \int_0^1 x e^{-2\pi i\nu x}\, dx - \int_0^1 e^{-2\pi i\nu x} dx \\
&= \left[-\frac{1}{2\pi i\nu}\, e^{-2\pi i\nu x} x\right]_0^1 - \frac{1}{2}\left[-\frac{1}{2\pi i\nu}\, e^{-2\pi i\nu x}\right]_0^1 + \frac{1}{2\pi i\nu}\int_0^1 e^{-2\pi i\nu x}\, dx \\
&= -\frac{1}{2\pi i\nu}\left[e^{-2\pi i\nu} - 0\right] - \frac{1}{2}\left[-\frac{1}{2\pi i\nu}\left(e^{-2\pi i\nu} - 1\right)\right] - \frac{1}{(2\pi i\nu)^2}\left[e^{-2\pi i\nu x}\right]_0^1 \\
&= -\frac{1}{2\pi i\nu} - \frac{1}{2}\cdot 0 - \frac{1}{(2\pi i\nu)^2}\cdot 0 = -\frac{1}{2\pi i\nu}
\end{aligned}$$

für $\nu = 0$ folgt:

$$c_0 = \int_0^1 \psi(x)\, dx = 0$$

also

$$\begin{aligned}
\psi(x) &= -\sum_{-\infty}^{+\infty}{}' \frac{1}{2\pi i\nu}\, e^{2\pi i\nu x} \\
&= -\sum_{\nu=1}^{\infty} \frac{1}{2\pi i\nu}\left(e^{2\pi i\nu x} - e^{-2\pi i\nu x}\right) \\
&= -\sum_{\nu=1}^{\infty} \frac{1}{2\pi i\nu}\, 2i\sin 2\pi\nu x \\
&= -\frac{1}{\pi}\sum_{\nu=1}^{\infty} \frac{\sin 2\nu\pi x}{\nu}
\end{aligned}$$

Wir führen nun als Hilfsfunktionen ein:

$$\psi_\mu(x) = \frac{1}{(2\pi i)^p} \sum_{-\infty}^{\infty}{}' \frac{e^{2\pi i\nu x}}{\nu^\mu}, \quad \text{sodaß} \quad \psi_1(x) = -\psi(x)$$

und

$$\psi'_\mu(x) = \frac{1}{(2\pi i)^p} \sum_{-\infty}^{+\infty} 2\pi i\nu \, \frac{e^{2\pi i\nu x}}{\nu^\mu} = \psi_{\mu-1}(x)$$

Differentiation für $\mu > 1$ zulässig, da gleichmäßig konvergent.

Damit wird: I, 9

$$\int_0^n \psi(x) f'(x)\, dx = -\int_0^n \psi_1(x) f'(x)\, dx$$

$$\begin{aligned}
&= -\psi_2 f'\Big|_0^n + \int_0^n \psi_2(x) f''(x)\, dx \\
&= \Big[-\psi_2 f' + \psi_3 f''\Big]_0^n - \int_0^n \psi_3 f'''\, dx \\
&\quad \cdots\cdots\cdots\cdots\cdots\cdots \\
&= \Big[-\psi_2 f' + \psi_3 f'' - \cdots\cdots + (-1)^{k-1}\psi_k f^{(k-1)}\Big]_0^n + (-1)^k \int_0^n \psi_k f^{(k)}\, dx
\end{aligned}$$

$$\psi_\mu(0) = \frac{1}{(2\pi i)^\mu} \sum_{-\infty}^{+\infty}{}' \frac{1}{\nu^\mu} = \begin{cases} 0\,, & \text{wenn } \mu \text{ ungerade,} \\ \frac{2}{(2\pi i)^\mu}\,\zeta(\mu)\,, & \text{wenn } \mu \text{ gerade.} \end{cases}$$

Nun ist für gerades μ

$$\zeta(\mu) = \mathsf{B}_\mu \cdot (-1)^{\frac{\mu}{2}+1} \frac{1}{2\mu!\,(2\pi)^{-\mu}}$$

also

$$\frac{2}{(2\pi i)^\mu}\,\zeta(\mu) = -\frac{\mathsf{B}_\mu}{\mu!}\,,$$

wo B_μ die μ–te Bernoullische Zahl:

$$\mathsf{B}_1 = \frac{1}{2},\ \mathsf{B}_2 = \frac{1}{6},\ \mathsf{B}_3 = 0,\ \mathsf{B}_4 = -\frac{1}{30},\ \ldots$$

Daher:

$$\psi_\mu(0) = \begin{cases} 0\,, & \text{wenn } \mu \text{ ungerade} \\ -\frac{\mathsf{B}_\mu}{\mu!}\,, & \text{wenn } \mu \text{ gerade} \end{cases}$$

oder, da $\mu = 1$ gar nicht in Betracht kommt:

$$\psi_\mu(0) = -\frac{\mathsf{B}_\mu}{\mu!}\,; \quad (\mu \geqq 2)$$

I, 10 Da die $\psi_\mu(x)$ periodisch, ist dies auch der Wert von $\psi_\mu(n)$. Damit ergibt sich:

$$\int_0^n \psi(x) f'(x)\,dx = \sum_{\mu=2}^{k} (-1)^{\mu-1} \frac{(-\mathsf{B}_\mu)}{\mu!} \left[f^{(\mu-1)}(n) - f^{(\mu-1)}(0)\right] + (-1)^k \int_0^n \psi_k(x) f^{(k)}(x)\,dx$$

$$= \sum_{\mu=2}^{k} (-1)^{\mu} \frac{\mathsf{B}_\mu}{\mu!} \left[f^{(\mu-1)}(n) - f^{(\mu-1)}(0)\right] + (-1)^k \int_0^n \psi_k(x) f^{(k)}(x)\,dx$$

und somit

$$\sum_{\nu=0}^{n} f(\nu) = \int_0^n f(x)\,dx + \frac{f(0)+f(n)}{2} + \sum_{\mu=2}^{k} \frac{(-1)^\mu \mathsf{B}_\mu}{\mu!} \left[f^{(\mu-1)}(n) - f^{(\mu-1)}(0)\right] + (-1)^k \int_0^n \psi_k(x) f^{(k)}(x)\,dx$$

Diese Formel heißt *Eulersche Summenformel.* Sie gilt unter der Voraussetzung eines für $0 \leqq x \leqq n$ stetigen, mindestens k–mal differentierbaren $f(x)$ für jedes positive ganze n und $k \geqq 1$. Wegen $\mathsf{B}_1 = \frac{1}{2}$ kann man sie auch eleganter so schreiben:

$$\sum_{\nu=0}^{n} f(\nu) = \int_0^n f(x)\,dx + f(n) + \sum_{\mu=1}^{k} \frac{(-1)^\mu \mathsf{B}_\mu}{\mu!}\left[f^{(\mu-1)}(n) - f^{(\mu-1)}(0)\right]$$
$$+(-1)^k \int_0^n \psi_k(x) f^{(k)}(x)\,dx$$

Zur Gewinnung der *Stirlingschen Formel* und *Stirlingschen Reihe* setzen wir $f(x) = \lg x$ und nehmen als untere Summationsgrenze 1, was offenbar durch sinngemäße Änderung des Beweises und der Formel gestattet. Die höheren Ableitungen von $\lg x$ sind offenbar

$$f(x) = \lg x\,, \quad f'(x) = \frac{1}{x}\,, \quad f''(x) = -\frac{1}{x^2}\,, \ldots,$$
$$f^{(\mu)}(x) = (-1)^{\mu-1}\frac{(\mu-1)!}{x^\mu}$$

Also wird: I, 11

$$\begin{aligned} f^{(\mu-1)}(n) - f^{(\mu-1)}(1) &= \frac{(-1)^\mu(\mu-2)!}{n^{\mu-1}} - \frac{(-1)^\mu(\mu-2)!}{1} \\ &= (-1)^\mu(\mu-2)!\left[\frac{1}{n^{\mu-1}} - 1\right] \end{aligned}$$

und somit

$$\sum_{\nu=1}^{n} \lg x = \lg n! = \int_1^n \lg x\,dx + \frac{0+\lg n}{2} + \sum_{\mu=2}^{k}\frac{\mathsf{B}_\mu}{\mu(\mu-1)}\left(\frac{1}{n^{\mu-1}} - 1\right)$$
$$-\int_1^n \psi_k(x)\frac{(k-1)!}{x^k}\,dx$$

$$\lg n! = n\lg n - n + 1 + \frac{1}{2}\lg n + \sum_{\mu=2}^{k}\frac{\mathsf{B}_\mu}{\mu(\mu-1)}\left(\frac{1}{n^{\mu-1}} - 1\right)$$
$$-(k-1)!\int_1^n \frac{\psi_k(x)}{x^k}\,dx$$

Nun ist nach der *als bekannt vorauszusetzenden* ersten Approximation der Stirlingschen Formel:

$$\lim_{n=\infty}\left[\lg n! - n\lg n + n - \frac{1}{2}\lg n\right] = \frac{1}{2}\lg 2\pi$$

Folglich ist

$$\frac{1}{2}\lg 2\pi = 1 - \sum_{\mu=2}^{k}\frac{\mathsf{B}_\mu}{\mu(\mu-1)} - (k-1)!\int\limits_1^\infty \frac{\psi_k(x)}{x^k}\,dx$$

(**Anm**. Man könnte vielleicht diese Formel für den Wert $\int\limits_1^\infty \frac{\psi_k(x)}{x^k}\,dx$ *direkt* beweisen, indem man das Integral auszuwerten sucht).

Setzt man hieraus den Wert für $\int\limits_1^n \frac{\psi_k(x)}{k^k}\,dx$ ein (subtrahiert beide Gleichungen), so folgt:

I, 12

$$\boxed{\lg n! = \lg\left(n^n e^{-n}\sqrt{2\pi n}\right) + \sum_{\mu=2}^{k}\frac{\mathsf{B}_\mu}{\mu(\mu-1)}\,\frac{1}{n^{\mu-1}} + (k-1)!\int\limits_n^\infty \frac{\psi_k(x)}{x^k}\,dx}$$

Dies ist die *Stirlingsche Formel*. Das Restglied ist wegen der Periodizität von $\psi_k(x)$ in n von der Ordnung $\int\limits_n^\infty \frac{1}{x^k}\,dx = O\left(\frac{1}{n^{k-1}}\right)$. Während also für $k \to \infty$ die rechte Seite divergieren würde, ist *für festes* n die Annäherung an $\lg n!$ sogar mit n^{k-1} multipliziert noch beschränkt. Die abgeleitete Formel hat daher den Charakter einer *asymptotischen Entwicklung* im Poincaréschen Sinne.

Durch Anwendung der Eulerschen Summenformel auf die für *alle* komplexen x gültige Formel

$$\log\Gamma(x+1) = \lim_{n=\infty}\left(\sum_{\nu=1}^{n}\lg\nu + x\lg n - \sum_{\nu=1}^{n}\lg(x+\nu)\right)$$

(Gaussscher limes), und zwar sowohl auf die erste Summe, als auch auf die zweite, unter Verwendung der obigen Formel entsteht dann leicht eine ganz ähnlich gebaute Formel für $\lg\Gamma(x+1)$, die für beliebiges komplexes x gilt.

Auch kann man aus der Eulerschen Summenformel in der Gestalt auf S. 7] durch Einführung der Fourier Reihe für $\psi(x)$ und gliedweise Integration die *Dirichletsche Summenformel* erhalten. Zur Ermöglichung der gliedweisen Integration muß jedoch erst durch partielle Integration $\psi_2(x)$ eingeführt werden. Jedoch ist wohl folgender Weg zur Herleitung bequemer: I, 13

Gegeben eine komplexe Funktion $f(t)$, sodaß $\sum\limits_{n=-\infty}^{+\infty} f(n)$ konvergiert. Dann ist

$$\varphi(v) = \sum_{n=-\infty}^{+\infty} f(n+v)$$

eine periodische Funktion in v mit der Periode 1. Ist also f „vernünftig“, so existiert die Fourier–Entwicklung

$$\begin{aligned}
\varphi(v) &= \sum_{\nu=-\infty}^{+\infty} e^{2\pi i\nu v} \int_0^1 \varphi(t)\, e^{-2\pi i\nu t}\, dt \\
&= \sum_{\nu=-\infty}^{+\infty} e^{2\pi i\nu v} \int_0^1 \sum_{n=-\infty}^{+\infty} f(n+t)\, e^{-2\pi i\nu t}\, dt \\
&= \sum_{\nu=-\infty}^{+\infty} e^{2\pi i\nu v} \sum_{n=-\infty}^{+\infty} \int_0^1 f(n+t)\, e^{-2\pi i\nu t}\, dt \\
&= \sum_{\nu=-\infty}^{+\infty} e^{2\pi i\nu v} \sum_{n=-\infty}^{+\infty} \int_n^{n+1} f(t)\, e^{-2\pi i\nu t}\, dt \\
&= \sum_{\nu=-\infty}^{+\infty} e^{2\pi i\nu v} \int_{-\infty}^{\infty} f(t)\, e^{-2\pi i\nu t}\, dt
\end{aligned}$$

Speziell also:

$$\sum_{n=-\infty}^{+\infty} f(n) = \varphi(0) = \sum_{\nu=-\infty}^{+\infty} \int_{-\infty}^{+\infty} f(t)\, e^{-2\pi i\nu t}\, dt$$

Dirichletsche Summenformel

I, 14

Angewendet auf $f(t) = e^{-\pi x t^2}$ ergibt sie:

$$\begin{aligned}\vartheta(x) &= \sum_{n=-\infty}^{+\infty} e^{-\pi x n^2} = \sum_{\nu=-\infty}^{+\infty} \int_{-\infty}^{+\infty} e^{-\pi x t^2 - 2\pi i \nu t}\, dt \\ &= \sum_{\nu=-\infty}^{+\infty} \int_{-\infty}^{+\infty} e^{-\pi x (t^2 + 2 i \nu \frac{t}{x} - \frac{\nu^2}{x^2}) - \frac{\pi \nu^2}{x}}\, dt \\ &= \sum_{\nu=-\infty}^{+\infty} e^{-\frac{\pi\nu^2}{x}} \int_{-\infty}^{+\infty} e^{-\pi x (t + \frac{i\nu}{x})^2}\, dt\end{aligned}$$

Ersetzt man $t + \frac{i\nu}{x} = u$, so geht der Integrationsweg in eine Parallele zur reellen Achse über, darf aber wegen der absoluten und gleichmäßigen Konvergenz in die reelle Achse zurückverschoben werden:

$$\begin{aligned}\vartheta(x) &= \sum_{\nu=-\infty}^{+\infty} e^{-\frac{\pi\nu^2}{x}} \int_{-\infty}^{+\infty} e^{-\pi x u^2}\, du \\ &= \sum_{\nu=-\infty}^{+\infty} e^{-\frac{\pi\nu^2}{x}} \cdot \frac{1}{\sqrt{\pi x}} \int_{-\infty}^{+\infty} e^{-v^2}\, dv\,,\end{aligned}$$

wenn $\sqrt{\pi x}$ für positives x positiv ist. Schließlich ist, wenn

$$J = \int_{-\infty}^{+\infty} e^{-v^2}\, dv$$

gesetzt wird

$$J^2 = \int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} e^{-(u^2+v^2)}\, du\, dv$$

Dies geht durch $\left\{\begin{array}{l} u = r\cos\varphi \\ v = r\sin\varphi \end{array}\right\}$, also $\dfrac{\partial(u,v)}{\partial(r,\varphi)} = r$ über in

$$J^2 = \int_0^\infty \int_0^{2\pi} e^{-r^2}\, d\varphi\, r dr = 2\pi \int_0^\infty e^{-r^2} r dr$$
$$= \pi \int_0^\infty e^{-t}\, dt = \pi$$

also $J = \sqrt{\pi}$ (positiv). Somit wird: I, 15

$$\vartheta(x) = \frac{1}{\sqrt{x}}\,\vartheta\left(\frac{1}{x}\right)$$

und dies ist die bekannte Thetatransformationsformel aus der Theorie der elliptischen Funktionen.

1.3 Bemerkung über Klassenkörper der komplexen Multiplikation. (17.7.1923)

In the summer semester 1923 Hasse is lecturing on Takagi's class field theory (2 hours weekly) at the University of Kiel. (He had been informed earlier by Artin about Takagi's class field paper [Tak20]*; see Honda's Takagi-biography* [Hon76]*.) In this entry Hasse notes how the classical theory of complex multiplication can be derived from Takagi's class field theory. The date of this entry is immediately after Artin's visit to Hasse in Kiel. It appears that on this occasion Artin has mentioned this to Hasse. As a student Hasse had attended a course on complex multiplication by Hecke in Göttingen 1920/21, and he continued to be very interested in this throughout his life. He presented the theory in detail in Part I of his Klassenkörperbericht* [Has26a]. *In the same year 1926 he published a new approach to the theory of complex multiplication* [Has26b].

(Dr. Artin, 17. VII. 23.)

Jeder Zahlring in einem imaginär quadratischen Zahlkörper kann nach einem rationalen Modul definiert werden. Wenn auch im allgemeinen der Führer ein beliebiges Ideal ist, so betrachtet man als eigentlichen Führer den kleinsten rationalen Modul, nachdem er definiert werden kann.

Man erhält den einem solchen Ring entsprechenden Ringklassenkörper, wenn man aus jeder der Ringklassen ein reguläres (zum Führer primes) Ideal auswählt und durch eine Basis von Ringzahlen darstellt:

$$j = (\alpha, \beta)$$

Setzt man dann in die absolute Invariante $J(\tau)$ für τ die Basisquotienten $\frac{\alpha}{\beta}$ ein, so zeigt man vermöge der Invarianzeigenschaften von $J(\tau)$ leicht, daß $J\big(\frac{\alpha}{\beta}\big)$ erstens von der Wahl der Basiszahlen, zweitens von der Wahl von j innerhalb seiner Klasse unabhängig ist. Die den h Ringklassen entsprechenden h Werte $J\big(\frac{\alpha}{\beta}\big)$ sind dann die Wurzeln einer relativ Abelschen Gleichung h–ten Grades, die den Ringklassenkörper zum imaginär–quadratischen Körper in Bezug auf den ausgewählten Ring liefert.

I, 16

Um den allgemeinsten Strahlklassenkörper zu bekommen, muß man noch die absolut–Abelschen Zahlen (Einheitswurzeln) und gewisse Teilwerte der $\wp$–Funktion hinzunehmen, die aus der komplexen Multiplikation der elliptischen

Funktionen entspringen. Man kann dann ganz allgemein jeden Strahlklassenkörper allein durch die Exponentialfunktion und die Teilwerte der $\wp$ Funktion des Periodenverhältnisses $\sqrt{-d}$ für gewisse Argumente erhalten.

1.4 Zum Fermatschen Satz. (21.7.1923)

We see that already in 1923, Hasse was applying reciprocity laws to Fermat's equation $a^\ell + b^\ell = c^\ell$*. In particular, he derives the criterion of Wieferich* [Wie09] *and Furtwängler* [Fur12] *from the reciprocity law of* ℓ*-th powers. Later, Hasse will include this in the second volume of his class field report* [Has30b].

I, 17

21. VII. 23.

Sind a, b, c drei ganze, zu ℓ prime, teilerfremde Zahlen, die der Fermatschen Gleichung

$$a^\ell + b^\ell = c^\ell$$

genügen, so folgt, daß die Zahlen aus k_ζ (zu ℓ prim):

$$a + b,\ a + b\zeta,\ \dots\ a + b\zeta^{\ell-1}$$

sämtlich ℓ–te Idealpotenzen sind. Jedes Legendresche Symbol nach einem dieser Moduln muß identisch 1 sein.

$$\left(\frac{\zeta}{a+b}\right) = 1 \qquad \text{ergibt} \qquad \frac{N(a+b)-1}{\ell} \equiv 0 \ \text{mod.}\ \ell$$

also

$$\boldsymbol{(a+b)^{\ell-1} - 1 \equiv 0 \quad \text{mod } \ell^2.}$$

$\left(\frac{\zeta}{a+b\zeta}\right) = 1$ ergibt:

$$\frac{N(a+b\zeta)-1}{\ell} \equiv 0 \ \text{mod.}\ \ell$$

$$a^{\ell-1} + a^{\ell-2}b + \dots + b^{\ell-1} - 1 \equiv 0 \quad \text{mod } \ell^2$$

also

$$\frac{a^\ell + b^\ell}{a+b} \equiv 1 \quad \text{mod } \ell^2$$

d. h. einerseits

$$\boldsymbol{c^\ell \equiv a + b \quad \text{mod } \ell^2}$$

andererseits

$$\boldsymbol{a(a^{\ell-1}-1)+b(b^{\ell-1}-1)\equiv 0 \mod \ell^2.}$$

Es wird sich gleich herausstellen, daß sogar jede der Klammern für sich mod ℓ^2 verschwinden muß und noch etwas mehr. Es muß nämlich auch jeder der zu ℓ primen Zahlen

I, 18

$$\gamma_i = \frac{a+b\zeta^i}{a+b}\ ; \quad (i = 1, 2, \ldots \ell - 1)$$

mit der Entwicklung:

$$\gamma_i = 1 - \frac{b}{a+b}(1-\zeta^i) = 1 - u\lambda_i$$

wo $\frac{b}{a+b} = u$, $1-\zeta^i = \lambda_i$ gesetzt ist, ℓ–te Idealpotenz sein.

Ist nun p irgendeine in b aufgehende Primzahl, und f der Grad ihrer Primideale in k_ζ, so ist $p^f \equiv 1 \mod \ell$, ferner

$$\left(\frac{\gamma_i}{p^f}\right) = \left(\frac{\gamma_i}{p}\right)^f = 1$$

da $\gamma_i = 1 - \delta p$ mit für den Bereich von p ganzem δ aus k_ζ gesetzt werden kann ($a+b$ ist prim zu b, also p), und

$$\left(\frac{1-\delta p}{p}\right) = \left(\frac{1}{p}\right) = 1$$

ist. Daher folgt nach dem Reziprozitätsgesetz:

$$1 = \left(\frac{\gamma_i}{pf}\right)\left(\frac{p^f}{\gamma_i}\right)^{-1} = \zeta^{-i\mathsf{S}\left(\frac{\gamma_i-1}{\lambda_i}\cdot\frac{p^f-1}{\ell}\right)} = \zeta^{-i\mathsf{S}\left(-u\cdot\frac{p^f-1}{\ell}\right)}$$

also, wegen $u = \frac{b}{a+b} \not\equiv 0 \mod \ell$,

$$p^f - 1 \equiv 0 \mod \ell^2$$

Dies gilt für jeden Primteiler von a, b, c. Es gilt somit, wegen $f|\ell-1$ speziell

$$\begin{aligned} \boldsymbol{a^{\ell-1}-1} &\equiv \mathbf{0} \mod \boldsymbol{\ell^2} \\ \boldsymbol{b^{\ell-1}-1} &\equiv \mathbf{0} \mod \boldsymbol{\ell^2} \\ \boldsymbol{c^{\ell-1}-1} &\equiv \mathbf{0} \mod \boldsymbol{\ell^2} \end{aligned}$$

und da 2 stets in einer der drei Zahlen aufgeht

$$\mathbf{2^{\ell-1} - 1 \equiv 0 \mod \ell^2} \qquad \text{(Furtwängler, Wieferich).}$$

I, 19

Der Fermatsche Satz läßt sich zurückführen auf folgende
Behauptung: *Die Funktion*

$$f(u) = u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots + \frac{u^{\ell-1}}{\ell - 1}$$

verschwindet mod. ℓ *außer für* $u = 0, 1 \mod \ell$ *für kein* u.

Bildet man nämlich das Produkt der $\ell - 1$ Einseinheiten γ_i (die Norm), so folgt

$$\gamma = \gamma_1 \gamma_2 \cdots \gamma_{\ell-1} = (1 - u\lambda_1) \cdots (1 - u\lambda_{\ell-1})$$

also

$$\log \gamma = \sum_{i=1}^{\ell-1} \log \gamma_i = \sum_{i=1}^{\ell-1} \log(1 - u\lambda_i)$$

Nun ist

$$-\log(1 - u\lambda_i) \equiv u\lambda_i + \frac{u^2\lambda_i^2}{2} + \cdots + \frac{u^{\ell-1}\lambda_i^{\ell-1}}{\ell - 1} + \frac{u^\ell \lambda_i^\ell}{\ell} \mod \mathfrak{l}^\ell$$

und

beachte

$$\begin{aligned} 0 &= \log \zeta_i \\ &= \log(1 - \lambda_i) \end{aligned}$$

$$\begin{aligned} u\lambda_i + \frac{u^\ell \lambda_i^\ell}{\ell} &\equiv u\lambda_i \left(1 + \frac{\lambda_i^{\ell-1}}{\ell}\right) \equiv u\lambda_i(1 + \varepsilon_i) \\ &\equiv u\lambda_i \left(-\frac{\lambda_i}{2} - \frac{\lambda_i^2}{3} - \cdots - \frac{\lambda_i^{\ell-2}}{\ell - 1}\right) \mod \mathfrak{l}^\ell \end{aligned}$$

somit

$$-\log(1 - u\lambda_i) \equiv \frac{u^2 - u}{2}\, \lambda_i^2 + \frac{u^3 - u}{3}\, \lambda_i^3 + \cdots + \frac{u^{\ell-1} - u}{\ell - 1}\, \lambda_i^{\ell-1}$$

und

beachte $S(\lambda_i^\nu) = \ell$

$$
\begin{aligned}
-\log(\gamma) &\equiv \left(\frac{u^2-u}{2} + \frac{u^3-u}{3} + \cdots + \frac{u^{\ell-1}-u}{\ell-1}\right)\ell \mod \mathfrak{l}^{\ell} \\
&\equiv \left(u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots + \frac{u^{\ell-1}}{\ell-1}\right)\ell \equiv 0 \mod \ell^2
\end{aligned}
$$

da $-\log\gamma$ rational. Es ist nämlich

$$
\gamma = \frac{a^\ell + b^\ell}{(a+b)^\ell} = \left(\frac{c}{a+b}\right)^\ell
$$

Da nun $c \equiv a+b \mod \ell$, ist γ die ℓ–te Potenz einer Einseinheit für ℓ und daher $\equiv 1 \mod \ell^2$, also sein Logarithmus

I, 20

$$
\log\gamma \equiv 0 \mod \ell^2
$$

Es genügt also, obige Behauptung zu beweisen ($u \equiv 0, 1 \mod \ell$ entspricht a oder $b \equiv 0 \mod \ell$). Man kommt auf diese Form auch ohne Logarithmen so:

Es müßte sein:

$$
\left(\frac{c}{a+b}\right)^\ell = \left(\frac{a}{a+b}\right)^\ell + \left(\frac{b}{a+b}\right)^\ell = (1-u)^\ell + u^\ell \equiv 1 \mod \ell^2
$$

also

$$
\begin{gathered}
\frac{\left(\frac{c}{a+b}\right)^\ell - 1}{\ell} = \frac{(1-u)^\ell + u^\ell - 1}{\ell} \equiv 0 \mod \ell \\
\frac{1 - \binom{\ell}{1}u + \binom{\ell}{2}u^2 - \cdots - u^\ell + u^\ell - 1}{\ell} \\
= -u + \frac{\binom{\ell}{2}}{\ell}u^2 - \frac{\binom{\ell}{3}}{\ell}u^3 \cdots + \frac{\binom{\ell}{\ell-1}}{\ell}u^{\ell-1}.
\end{gathered}
$$

Nun ist

$$
\frac{\binom{\ell}{\nu}}{\ell} = \frac{(\ell-1)(\ell-2)\cdots\big(\ell-(\nu-1)\big)}{1\cdot 2\cdots\nu} \equiv (-1)^{\nu-1}\frac{1}{\nu}
$$

und somit obiger Ausdruck

$$
\equiv -\left(u + \frac{u^2}{2} + \frac{u^3}{3} + \cdots + \frac{u^{\ell-1}}{\ell-1}\right) \text{ mod. } \ell
$$

Zum Beweis des Fermatschen Satzes (Fall I) würde folgender Gedankengang von Vorteil sein:

Sind $\alpha = 1 + v\lambda^h$, $\beta = 1 + w\lambda^k$ zwei zueinander prime Zahlen aus k_ζ, für die $h + k = \ell$ ist und beide ℓ–te Idealpotenzen, so folgt (nach Kummer–Takagi):

$$1 = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\pm h\,\mathsf{S}(vw)},$$

also können nicht beide Zahlen v, w Einheiten für $\mathfrak{l}$ sein. Nun kann man einerseits aus den obigen Zahlen γ_i eine Reihe ℓ–ter Idealpotenzen multiplikativ zusammensetzen, z. B. eine Einseinheit zweiten Grades so:

I, 21

$$\gamma_1 = \frac{a+b\zeta}{a+b} = 1 - \frac{b}{a+b}\,\lambda$$

$$\frac{1}{\gamma_2} = \frac{a+b}{a+b\zeta^2} = 1 + \frac{b}{a+b\zeta^2}(1-\zeta^2)$$

$$= 1 + \frac{b}{a+b\zeta^2}\lambda(2-\lambda) = 1 + \frac{2b}{a+b\zeta^2}\,\lambda - \frac{b}{a+b\zeta^2}\,\lambda^2$$

Es ist weiter

$$\begin{aligned} \frac{1}{a+b\zeta^2} &= \frac{1}{a+b} + \frac{1}{a+b\zeta^2} - \frac{1}{a+b} \\ &= \frac{1}{a+b} + \frac{b\lambda(2-\lambda)}{(a+b\zeta^2)(a+b)} \\ &\equiv \frac{1}{a+b} + \frac{2b}{(a+b)^2}\,\lambda + \cdots - \end{aligned}$$

also

$$\begin{aligned} \frac{1}{\gamma_2} &= 1 + \frac{2b}{a+b}\,\lambda + \frac{4b^2 - b(a+b)}{(a+b)^2}\,\lambda^2 + \cdots \\ \gamma_1^2 &= 1 - \frac{2b}{a+b}\,\lambda + \frac{b^2}{(a+b)^2}\,\lambda^2 \end{aligned}$$

$$\begin{aligned} \frac{\gamma_1^2}{\gamma_2} &= 1 - \frac{4b^2}{(a+b)^2}\,\lambda^2 + \frac{4b^2 - b(a+b)}{(a+b)^2}\,\lambda^2 + \frac{b^2}{(a+b)^2}\,\lambda^2 + \cdots \\ &= 1 - \frac{ab}{(a+b)^2}\,\lambda^2 + \cdots \end{aligned}$$

(NB. Im Falle II wird dies $\equiv 1 \mod. \lambda^3$, daher nicht verwendbar)

Andererseits hat man als ℓ–te Idealpotenzen die Einheiten von k_ζ zur Verfügung nämlich

1.) Die Einheitswurzeln ζ nebst konjugierten

2.) Die Einheiten $\varepsilon_i = \frac{\lambda_i^{\ell-1}}{\ell} \equiv -1 - \frac{\lambda_i}{2} - \frac{\lambda_i^2}{3} - \cdots - \frac{\lambda_i^{\ell-2}}{\ell-1} \mod \ell$

3.) Die Einheiten
$$\eta_k = \frac{\lambda_k}{\lambda} = 1 + \zeta + \cdots + \zeta^{k-1}$$

I, 22

Einseinheiten für $\mathfrak{l}$ sind nur die ersten beiden Kategorien, die letzte erst in der $(\ell - 1)$ ten Potenz. Aus diesen kann man multiplikativ Einseinheiten höheren Grades zusammensetzen, z. B.

$$\begin{aligned} -\varepsilon &= 1 + \frac{\lambda}{2} + \frac{\lambda^2}{3} + \cdots \\ \varepsilon^2 &= 1 + \lambda + \frac{11}{12}\lambda^2 + \cdots \\ \zeta &= 1 - \lambda \end{aligned}$$

$$\zeta\varepsilon^2 = 1 - \frac{1}{12}\lambda^2 + \cdots$$

Gelingt es auf diese Weise eine Einheit zu konstruieren, die den Typus $1 - \delta\lambda^{\ell-3}$ hat, wo δ prim zu $\mathfrak{l}$ ist, so könnte man mit einer entsprechend aus den γ_i konstruierten Einheit den Fermatschen Satz beweisen. Selbstverständlich sind Einheit des Typus $1 - \delta\lambda^{\ell-2}$, $1 - \delta\lambda^{\ell-1}$ unmöglich, womit sie nach dem Reziprozitätsgesetz mit ζ, $\varepsilon^2\zeta$ zum Widerspruch führen würden. Dagegen liegt auf Grund des Satzes 155 (S. 438) des Zahlberichts die Möglichkeit nahe, daß auch im *beliebigen* Kreiskörper $1 - \delta\lambda^{\ell-3}$ erreicht werden kann.

1.5 Die Kummerschen logarithmischen Differentialquotienten. (21.7.1923)

Kummer introduced his logarithmic differential quotients for studying cyclotomic units, both in connection with reciprocity laws and Fermat's Last Theorem. Here, Hasse gives a definition that is more conceptual than the one given in Hilbert's Zahlbericht. Later, Hasse studied the Kummer logarithmic differential quotients in his Crelle paper [Has25c] *and compared them with the logarithms in the sense of Hensel. See also the joint paper of Hasse with Artin* [AH25] *in the same volume of Crelle's Journal. For a modern presentation see the section on logarithmic derivatives in Washington* [Was82] §13.7. *See also the entry 3.5 of May, 27, 1934 in Book III.]*

I, 23

21. VII. 23.

Sei $\alpha = \varphi(\zeta)$ eine für den Bereich von ℓ ganze Zahl des Kreiskörpers k_ζ und $\alpha \equiv 1 \mod \mathfrak{l}$, also $\varphi(1) \equiv 1$ mod. ℓ, dann definiert man die *logarithmischen Differentialquotienten* $\ell^{(\nu)}(\alpha)$ für $\nu = 1, 2, \ldots, \ell - 1$ folgendermaßen:

Man entwickle die ganze rationale Funktion $\varphi(x)$ für $x = e^v$ in eine logarithmische Potenzreihe:

$$\log \varphi(e^v) = c_0 + \frac{c_1}{1!}\, v + \frac{c_2}{2!}\, v^2 + \cdots + \frac{c_{\ell-1}}{(\ell-1)!}\, v^{\ell-1} + \cdots \tag{1}$$

NB. Für den Beweis ist es angebracht, mit den rationalen Ausdrücken $\frac{x\varphi^2(x)}{\varphi(x)}$, $\frac{x^2\varphi(x)\varphi(x)+x\varphi'(x)\varphi(x)-x^2\varphi'(x)^2}{\varphi(x)^2}$, ... zu arbeiten!

Satz: *Die Koeffizienten* $c_1, c_2, \ldots, c_{\ell-2}$ *sind* mod. ℓ *unabhängig von der speziellen Wahl von* $\varphi(\zeta)$, *der Koeffizient* c_0 *ist* $\equiv 0 \mod \ell$, *der Koeffizient* $c_{\ell-1}$ *ändert sich um* $+\frac{\varphi(1)-\psi(1)}{\ell}$, *wenn* $\varphi(\zeta)$ *durch* $\psi(\zeta)$ *ersetzt wird.*

Beweis: Daß $c_0 \equiv 0 \mod \ell$ folgt aus

$$c_0 = \log \varphi(e^0) = \log \varphi(1) = \log(1 + k\ell) = k\ell + \cdots .$$

Ist ferner $\psi(\zeta)$ eine andere Darstellung für α, so gilt

$$\varphi(x) = \psi(x) + g(x)(x^{\ell-1} + \cdots + x + 1)$$

mit ganzem $g(x)$. Für $x = e^v$ folgt:

$$\varphi(e^v) = \psi(e^v) + g(e^v)\left[\ell + \sum_{i=1}^{\infty} \frac{v^i}{i!} \sum_{\nu=1}^{\ell-1} \nu^i\right]$$

Wegen $\sum_{\nu=1}^{\ell-1} \nu^i \equiv 0 \bmod. \ell$ für $i = 1, \dots \ell - 2$ und $\equiv -1 \bmod. \ell$ für $i = \ell - 1$ folgt, daß die Klammer von der Form I, 24

$$\left[v^{\ell-1} + (v^\ell) + (\ell)\right]$$

ist, wo (v^ℓ) höhere Potenzen und (ℓ) Vielfache von ℓ andeutet. Die Entwicklungen von $\varphi(e^v)$ und $\psi(e^v)$ unterscheiden sich also mod ℓ in ihren Koeffizienten von $1, v, \dots v^{\ell-2}$ nicht, während die Koeffizienten von $v^{\ell-1}$ so zusammenhängen:

$$a_{\ell-1} \equiv b_{\ell-1} + g(1) \bmod. \ell$$

$g(1)$ ergibt sich für $x = 1$ zu:

$$\frac{\varphi(1) - \psi(1)}{\ell}.$$

Ist nun dementsprechend

$$\begin{aligned} \varphi(e^v) &= 1 + a_1 v + \cdots + a_{\ell-1} v^{\ell-1} + (v^\ell) + (\ell) \\ \psi(e^v) &= 1 + b_1 v + \cdots + b_{\ell-1} v^{\ell-1} + (v^\ell) + (\ell) \end{aligned}$$

so folgt:

$$\begin{aligned} \log \varphi(e^v) &= \sum_{\nu=1}^{\infty} \frac{(-1)^\nu}{\nu} \left[a_1 v + \cdots + a_{\ell-1} v^{\ell-1} + (v^\ell) + (\ell)\right]^\nu \\ \log \psi(e^v) &= \sum_{\nu=1}^{\infty} \frac{(-1)^\nu}{\nu} \left[b_1 v + \cdots + b_{\ell-1} v^{\ell-1} + (v^\ell) + (\ell)\right]^\nu. \end{aligned}$$

Auf die ersten $\ell - 1$ Koeffizienten dieser Entwicklungen können erstens die Glieder (v^ℓ) keinen Einfluß haben, zweitens aber auch nicht die Glieder (ℓ), wenn man jene Koeffizienten nur mod. ℓ betrachtet. Denn man überzeugt sich leicht, daß trotz der Nenner ν auch in den späteren Gliedern der $\sum_\nu$ durch (ℓ) nur Glieder mit durch ℓ teilbarem Koeffizienten erzeugt werden. Wegen des Übereinstimmens der $a_1, \dots, a_{\ell-2}$ mit den $b_1, \dots, b_{\ell-2}$ mod. ℓ stimmen somit die Koeffizienten von $v, v^2, \dots v^{\ell-2}$ in beiden Entwicklungen mod. ℓ überein. Die Abweichung in $a_{\ell-1}$, $b_{\ell-1}$ kann sich nur im Glied $\nu = 1$ bemerkbar machen, da sie in späteren schon auf höhere Potenzen übertritt. Dieses Glied liefert als Koeffizient von $\frac{v^{\ell-1}}{(\ell-1)!}$: I, 25

$$+a_{\ell-1} \quad \text{bzw.} \quad + b_{\ell-1} \equiv +a_{\ell-1} - \frac{\varphi(1) - \psi(1)}{\ell} \bmod. \ell$$

sodaß also die Behauptung vollständig bewiesen ist.

Man nennt nun die Koeffizienten $c_1, c_2, \dots c_{\ell-2}$, *in* (1) *die eindeutig* mod. ℓ *bestimmt sind, die logarithmischen Differentialquotienten* $\ell^{(1)}(\alpha), \dots, \ell^{(\ell-2)}(\alpha)$. Den letzten dieser log. Diff. Qu. $\ell^{(\ell-1)}(\alpha)$ muß man durch geeignete Normierung definieren. Man kann nämlich zu jedem

$$\alpha = \varphi(\zeta)$$

eine Darstellung $\alpha = \psi(\zeta)$ finden, die der Bedingung

$$\psi(1) = 1$$

genügt, indem man die Funktion

$$\psi(x) = \varphi(x) + \frac{1-\varphi(1)}{\ell}\,(x^{\ell-1} + x^{\ell-2} + \cdots + x + 1)$$

nimmt. Dieses (oder jedes andere so beschaffene) $\psi(x)$ soll zur Normierung (Festlegung) von $\ell^{(\ell-1)}(x)$ benutzt werden, was nach obigem hierdurch eindeutig möglich ist. Es wird dann nach dem bewiesenen Satz

$$c_{\ell-1} \equiv \ell^{(\ell-1)}(\alpha) - \frac{1-\varphi(1)}{\ell} \ \text{mod.}\ \ell$$

also

$$\boldsymbol{\ell^{(\ell-1)}(\alpha) \equiv c_{\ell-1} + \frac{\varphi(1)-1}{\ell}}$$

sodaß auch $\ell^{(\ell-1)}(\alpha)$ aus der Reihenentwicklung für irgendein $\varphi(\zeta) = \alpha$ ohne weiteres abgelesen werden kann. I, 26

Aus dem Bewiesenen folgt unmittelbar, daß für zwei Zahlen α, β mit

$$\alpha \equiv \beta \quad \text{mod}\ \ell$$
$$\alpha \equiv \beta \equiv 1 \quad \text{mod}\ \mathfrak{l}$$

sämtliche log. Diff. Qu. bis zum $(\ell-2)$–ten mod ℓ kongruent sind. Denn die zugehörigen Funktionen $\varphi(x)$, $\psi(x)$ unterscheiden sich nur um Vielfache von ℓ und $x^{\ell-1} + \cdots + x + 1$, daß der obige Beweis direkt übertragen werden kann. Also:

Satz: *Es ist*

$$\ell^{(\nu)}(\alpha) \equiv \ell^{(\nu)}(\beta) \ \text{mod.}\ \ell, \quad \textit{wenn}$$
$$\alpha \equiv \beta \ \text{mod.}\ \ell \qquad\qquad (\nu = 1, 2, \dots \ell-2)$$

(Für $\nu = \ell - 1$ siehe folgende Seite]).

Ich untersuche ferner, wie sich $\ell^{(\nu)}(\alpha)$ ändert, wenn die erzeugende Substitution $s = (\zeta : \zeta^r)$ auf α angewendet wird. Dann gehört offenbar zu $s\alpha$ die Funktion $\varphi(x^r)$, die in der Tat für $x = \zeta$ in $\varphi(\zeta^r)$, d. h. das aus $\alpha = \varphi(\zeta)$ durch s entstehende $s\alpha$ übergeht. Entwickelt man also zunächst $\varphi(e^{vr})$ nach Potenzen von vr, so entstehen die logarithmischen Diff. Qu. von α als Koeffizienten der Potenzen von vr, während die log. Diff. Qu. von $s\alpha$ die Koeffizienten der Potenzen von v allein sind. Wegen der Übereinstimmung von $\varphi(1)$ für α und $s\alpha$ wird daher:

$$\boldsymbol{\ell^{(\nu)}(s\alpha) \equiv r^{\nu}\ell^{(\nu)}(\alpha) \ \textbf{mod.}\,\ell}\,; \qquad (\nu = 1, 2, \ldots, \ell - 1)$$

Ist ferner $\alpha = \varphi(\zeta)$, $\beta = \psi(\zeta)$ so erhält man die log. Diff. Qu. von $\alpha\beta$ durch Entwicklung von

$$\log\varphi(e^v)\psi(e^v) = \log\varphi(e^v) + \log\psi(e^v)\,.$$

Berücksichtigt man noch die für zwei ganz beliebige rationale Zahlen $a, b \equiv 1$ mod ℓ gültige Kongruenz I, 27

$$\frac{a-1}{\ell} + \frac{b-1}{\ell} \equiv \frac{ab-1}{\ell} \quad \text{mod } \ell$$

(angewendet hier auf $\varphi(1)$, $\psi(1)$), so folgt

$$\boldsymbol{\ell^{(\nu)}(\alpha\beta) \equiv \ell^{(\nu)}(\alpha) + \ell^{(\nu)}(\beta) \ \textbf{mod.}\,\ell}$$
$$(\nu = 1, 2, \ldots, \ell - 1)$$

Für $\nu = \ell - 1$ ist der Satz auf voriger Seite] oben nicht richtig, da die Normierungsglieder $\frac{\varphi(1)-1}{\ell}$ und $\frac{\psi(1)-1}{\ell}$ für $\alpha \equiv \beta$ mod. ℓ verschieden sein können. Ist aber dann sogar

$$\alpha \equiv \beta \quad \text{mod } \mathfrak{l}^{\ell}$$

und benutzt man die normierten Darstellungen:

$$\begin{aligned}
\alpha &= \varphi(\zeta) \\
\overline{\varphi}(x) &= \varphi(x) + \frac{1-\varphi(1)}{\ell}(1 + \cdots + x^{\ell-1}) \\
\beta = \psi(\zeta) &= \varphi(\zeta) + \ell\,\lambda g(\zeta) \\
\overline{\psi}(x) &= \psi(x) + \frac{1-\psi(1)}{\ell}(1 + \cdots + x^{\ell-1}) \\
&= \varphi(x) + \ell(1-x)g(x) + \frac{1-\varphi(1)}{\ell}(1 + \cdots + x^{\ell-1}) \\
&= \overline{\varphi}(x) + \ell(1-x)\,g(x)\,,
\end{aligned}$$

so unterscheiden sich dieselben nur um Vielfache von ℓ, sodaß die ihnen entsprechenden Koeffizienten von $v^{\ell-1}$ nach dem obigen Schluß mod. ℓ kongruent sind. Also gilt:

$$\boldsymbol{\ell^{(\ell-1)}(\alpha) \equiv \ell^{(\ell-1)}(\beta) \ \textbf{mod.}\ \ell\,,}$$
$$\text{wenn} \quad \boldsymbol{\alpha \equiv \beta \quad \textbf{mod}\ \mathfrak{l}^{\ell}.}$$

Hilbert beweist im Zahlbericht, S. 414 ff. für den $(\ell-1)$–ten log. Diff. Quot.:

I, 28

$$\boldsymbol{\ell^{(\ell-1)}(\alpha) \equiv -\tfrac{n(\alpha)-1}{\ell} \ \textbf{mod.}\ \ell} \quad \text{(Beweis S. 33]).}$$

Hieraus ergeben sich übrigens leicht alle Abweichungen in den entwickelten Sätzen für $\ell^{(\ell-1)}(\alpha)$.

1.6 Die Takagische Basis für den Kreiskörper. (22.7.1923)

Kummer had proved an ℓ-th power reciprocity law in the cyclotomic field of ℓ-th roots of unity, for regular primes ℓ. Furtwängler had used the theory of Hilbert class fields for generalizing Kummer's result to all odd primes, and Takagi had given another proof [Tak22]. *One of the essential ingredients of Takagi's proof was to work with a specially constructed basis of the group of units $\equiv 1 \bmod \mathfrak{l}$ in the field. This was new to Hasse since he, following Hensel* [Hen16], *had previously used another basis in order to describe the reciprocity law. In this entry, Hasse tries to understand the principal properties of Takagi's basis and how this leads to an essential simplification of the proof of the explicit formulas for the reciprocity law (including the so-called second supplement).*

22. VII. 23.

Um eine Basisdarstellung für die Nichtreste mod $\mathfrak{l}^{\ell+1}$ im Kreiskörper zu finden, die sich dem Reziprozitätsgesetz einfach anpaßt, geht Takagi so vor:

An die Basiszahlen $\kappa_1, \kappa_2, \ldots, \kappa_\ell$, sodaß für jedes $\alpha \equiv 1$ mod. $\mathfrak{l}$ im Kreiskörper gilt:

$$\alpha = \kappa_1^{e_1} \kappa_2^{e_2} \cdots \kappa_\ell^{e_\ell} \xi^\ell \quad (\mathfrak{l}),$$

werden folgende beiden Forderungen gestellt:

$$\begin{array}{lrcl} (1) & \kappa_a & \equiv & 1 - \lambda^a \mod \mathfrak{l}^{a+1} \\ (2) & \kappa_a^{s-r^a} & \equiv & 1 \mod \mathfrak{l}^{\ell+1} \end{array}$$

Die erste Forderung ist im Henselschen Sinne hinreichend dafür, daß die κ_a eine Basis für $k(\mathfrak{l})$ bilden, die zweite zielt auf die beabsichtigte Anwendung auf das Reziprozitätsgesetz hin; s bedeutet die erzeugende Substitution $\zeta : \zeta^r$ des Kreiskörpers. $\kappa_a^{s-r^a}$ verwandelt *natürlich* κ_a in eine Einseinheit höheren Grades, denn es ist

$$\begin{array}{ll} \kappa_a^s = s\kappa_a \equiv 1 - (s\lambda)^a & \equiv 1 - r^a\lambda^a \mod \mathfrak{l}^{a+1} \\ \kappa_a^{r^a} & \equiv 1 - r^a\lambda^a \mod \mathfrak{l}^{a+1}, \end{array}$$

weil $s\lambda = 1 - \zeta^r = \lambda \frac{1-\zeta^r}{1-\zeta} = \lambda(1 + \cdots + \zeta^{r-1}) = r\lambda \mod \mathfrak{l}^2$ ist. Gefordert wird also, daß die späteren Glieder in κ_a so gewählt werden, daß sie durch $\kappa_a^{s-r^a}$ bis λ^ℓ herausfallen.

I, 29

Die gestellten Forderungen werden befriedigt durch folgende Basis:

$$\begin{aligned}
\kappa_1 &= \zeta = 1-\lambda \\
\kappa_a &= (1-\lambda^a)^{-r^a(s-1)(s-r)\ldots(s-r^{r-1})(s-r^{r+1})\ldots(s-r^{\ell-2})} \\
&\qquad\qquad\qquad\qquad \text{für } a = 2,3,\ldots\ \ell-2 \\
&\qquad\qquad\qquad\qquad\qquad (\text{auch für } a=1) \\
\kappa_{\ell-1} &= 1+\ell = 1-\lambda^{\ell-1}-\frac{\lambda^\ell}{2}+\cdots \\
\kappa_\ell &= 1-\lambda^\ell.
\end{aligned}$$

Die Forderung (1) ist für κ_1, $\kappa_{\ell-1}$, κ_ℓ ersichtlich erfüllt, für die übrigen κ_a bedenke man, daß s angewendet auf λ^a nach dem Modul $\mathfrak{l}^{a+1}$ nichts anderes bedeutet, als den Übergang zu $r^a\lambda^a$. Es wird somit*)

$$\begin{aligned}
\kappa_a &\equiv (1-\lambda^a)^{-r^a \frac{s^{\ell-1}-1}{s-r^a}\Big|_{s=r^a}} \equiv (1-\lambda^a)^{-r^a(\ell-1)\,r^{a(\ell-2)}} \mod \mathfrak{l}^{a+1} \\
&\equiv (1-\lambda^a)^{+r^a\cdot r^{-a}} \equiv 1-\lambda^a \mod \mathfrak{l}^{a+1}.
\end{aligned}$$

Die Forderung (2) ist für κ_1 wegen $\zeta^{s-r}=1$ erfüllt, für $\kappa_{\ell-1}$ ebenso, für κ_ℓ wegen

$$\kappa_\ell^{s-r^\ell} \equiv \frac{1-r^\ell\lambda^\ell}{1-r^\ell\lambda^\ell} \equiv 1 \mod \mathfrak{l}^{\ell+1}.$$

Für die übrigen κ_a wird:

$$\kappa_a^{s-r^a} \equiv (1-\lambda^a)^{-r^a(s^{\ell-1}-1)} \equiv (1-\lambda^a)^{-r^a\cdot 0} \equiv 1 \mod \mathfrak{l}^{\ell+1}$$

Für die so gewählte Basis beweist Takagi dann leicht folgende Reziprozitätsgesetze:

$$\text{Ist}\qquad \begin{aligned}
\alpha &= \kappa_1^{e_1}\cdots\kappa_\ell^{e_\ell}\,\xi^\ell \quad (\mathfrak{l}) \\
\beta &= \kappa_1^{e_1'}\cdots\kappa_\ell^{e_\ell'}\,\xi'^\ell \quad (\mathfrak{l})
\end{aligned}$$

so ist:

$$\left(\frac{\boldsymbol{\alpha},\boldsymbol{\beta}}{\mathfrak{l}}\right)^{-1} = \left(\frac{\boldsymbol{\alpha}}{\boldsymbol{\beta}}\right)\left(\frac{\boldsymbol{\beta}}{\boldsymbol{\alpha}}\right)^{-1} = \boldsymbol{\zeta}^{-\sum_{a=1}^{\ell-1} a\,e_a\,e'_{\ell-a}}.$$

*) Vielfache von ℓ im Exponenten dürfen mod $\mathfrak{l}^{\ell+1}$ weggelassen werden!

In meinem Sinne ist also die den mittleren Basiszahlen $\kappa_1, \ldots, \kappa_{\ell-1}$ zugeordnete Matrix für $\left(\frac{\kappa_a, \kappa_b}{\mathfrak{l}}\right)$ (a Zeile, b Spalte):

	κ_1	κ_2	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\kappa_{\ell-2}$	$\kappa_{\ell-1}$
κ_1	0	0	$\cdots$	$\cdots$	$\cdots$	$\cdots$	0	1
κ_2	0					$\iddots$	2	0
$\vdots$	$\vdots$				$\iddots$	$\iddots$	$\iddots$	$\vdots$
$\vdots$	$\vdots$			$\iddots$	$\iddots$	$\iddots$		$\vdots$
$\vdots$	$\vdots$		$\iddots$	$\iddots$	$\iddots$			$\vdots$
$\vdots$	$\vdots$	$\iddots$	$\iddots$	$\iddots$				$\vdots$
$\kappa_{\ell-2}$	0	$\ell-2$	$\iddots$					$\vdots$
$\kappa_{\ell-1}$	$\ell-1$	0	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	0

Für den zweiten Ergänzungssatz folgt aus der natürlichen Basisdarstellung

$$\alpha = (1-\lambda)^{a_1}(1-\lambda^2)^{a_2}\cdots(1-\lambda^\ell)^{a_\ell}\,\xi^\ell \quad (\mathfrak{l})$$

das Gesetz:

$$\left(\frac{\lambda}{\alpha}\right) = \zeta^{a_\ell}.$$

In den Exponenten der κ_a–Basis findet man auf Grund der Eigenschaft (2) der Basis leicht:

$$\left(\frac{\ell}{\alpha}\right) = \zeta^{-e_\ell}$$

Dann wird $\left(\frac{\lambda}{\alpha}\right)$ in den e_a durch $\lambda^{\ell-1} = \ell\varepsilon$ ausgerechnet. Dazu sind die Exponenten von $\varepsilon = \frac{\lambda^{\ell-1}}{\ell}$ bei der κ_a–Darstellung anzugeben. Hierfür gilt nun ein allgemeines Prinzip, das die κ_a–Basis mit den log. Diff. Quot. in Verbindung bringt.

Die Exponenten e_a der κ_a–Basis sind nämlich im wesentlichen die log. Diff. Quot. Es ist nämlich einerseits:

$$
\begin{array}{lll}
 & \ell_\nu(\kappa_a^s) \equiv \ell_\nu(\kappa_a^{r^a}) \ \operatorname{mod.} \ell & (\nu = 1, 2, \dots \ell - 1) \\
\text{weil} & \kappa_a^s \equiv \kappa_a^{r^a} \quad \operatorname{mod} \mathfrak{l}^{\ell+1}, & \text{andererseits} \\
 & \ell_\nu(\kappa_a^s) \equiv r^\nu \ell_\nu(\kappa_a) & \text{nach S. 26].} \\
\text{Ferner} & \ell_\nu(\kappa_a^{r^a}) \equiv r^a \ell_\nu(\kappa_a) & \text{nach S. 27].}
\end{array}
$$

I, 31 also

$$r^a\, \ell_\nu(\kappa_a) \equiv r^\nu\, \ell_\nu(\kappa_a) \ \operatorname{mod.} \ell \qquad (\nu = 1, 2, \dots \ell - 1)$$

sodaß für $a \neq \nu$ folgt

$$\ell_\nu(\kappa_a) \equiv 0 \ \operatorname{mod.} \ell\,; \quad (a \neq \nu)$$

Für $a = \nu$ folgt

$$\ell_a(\kappa_a) \equiv \ell_a(1 - \lambda^a)^{-r^a(s-1)(s-r)\dots(s-r^{a-1})(s-r^{a+1})\dots(s-r^{\ell-2})}$$

Wegen $\ell_a(\alpha^s) \equiv r^a \ell_a(\alpha) \ \operatorname{mod.} \ell$ folgt, daß

$$\ell_a(\alpha^{F(s)}) \equiv F(r^a)\, \ell_a(\alpha) \ \operatorname{mod.} \ell$$

also

$$
\begin{aligned}
\ell_a(\kappa_a) \quad &\equiv \quad -r^a \left. \frac{s^{\ell-1} - 1}{s - r^a} \right|_{s=r^a} \ell_a(1 - \lambda^a) \\
&\equiv \quad \ell_a(1 - \lambda^a) \ \operatorname{mod.} \ell \qquad (a = 1, 2, \dots \ell - 2)
\end{aligned}
$$

Schließlich ist $\ell_a(1 - \lambda^a)$ so zu finden:

$$1 - \lambda^a = 1 - (1 - \zeta)^a$$

Funktion:

$$
\begin{aligned}
\varphi(\iota^\nu) \quad &= \quad 1 - (1 - \iota^\nu)^a \\
\log \varphi(\iota^\nu) \quad &= \quad -\sum_{\nu=1}^{\infty} \frac{(1 - \iota^\nu)^{a\nu}}{\nu} \\
(1 - \iota^\nu)^{a\nu} \quad &= \quad \sum_{\mu=0}^{a\nu} (-1)^\mu \binom{a\nu}{\mu} \iota^{\nu\mu}
\end{aligned}
$$

also

$$\log\varphi(\iota^\nu) = -\sum_{\nu=1}^{\infty}\frac{1}{\nu}\sum_{\mu=0}^{a\nu}(-1)^\mu\binom{a\nu}{\mu}\iota^{\nu\mu}$$

$$\ell_a(1-\lambda^a) = \left.\frac{d^a\big(\log\varphi(\iota^\nu)\big)}{d\nu^a}\right|_{\nu=0} = -\sum_{\nu=1}^{\infty}\frac{1}{\nu}\sum_{\mu=0}^{a\nu}(-1)^\mu\binom{a\nu}{\mu}\mu^a$$

Die $\sum_{\mu=0}^{a\nu}$ ist die $a\nu$–te Differenz der Reihe $0^a, 1^a, 2^a, \ldots$ also 0 falls $a\nu > a$, d. h. $\nu > 1$. Für $\nu = 1$ ist diese Differenz bekanntlich $(-1)^a a!$. Daher wird

$$\ell_a(1-\lambda^a) \equiv (-1)^{a-1}a! \ \text{mod.}\ \ell \qquad (a = 1, 2, \ldots \ell-1),$$

da $\varphi(1) = 1$ ist. I, 32

Wir beweisen jedoch eigentlich $a = \ell - 1$, was $\ell_{\ell-1}(1-\lambda^{\ell-1}) \equiv \ell_{\ell-1}(1+\ell) \equiv 1$ ergibt, nicht, da wir mit der Normdarstellung (S. 28]) auskommen. Letztere gibt in diesem Falle natürlich ebenfalls

$$\frac{1-n(1-\lambda^{\ell-1})}{\ell} \equiv \frac{1-n(1+\ell)}{\ell} \equiv 1 \mod \ell$$

Wir haben nunmehr gewonnen:

$$\boldsymbol{\ell_\nu(\kappa_a) \equiv 0 \quad \text{mod.}\ \ell \quad \text{für} \quad \nu \neq a}$$
$$\boldsymbol{\ell_\nu(\kappa_a) \equiv (-1)^{a-1}a! \quad \text{mod.}\ \ell \quad \text{für} \quad \nu = a}$$
$$(a, \nu = 1, 2, \ldots \ell - 1)$$

Bilden wir also in

$$\alpha \equiv \kappa_1^{e_1}\kappa_2^{e_2}\ldots\kappa_{\ell-1}^{e_{\ell-1}} \mod \ell\mathfrak{l} \tag{3}$$

beiderseits die logarithmischen Diff. Quotienten, so folgt:

$$\ell_\nu(\alpha) \equiv e_\nu\,\ell_\nu(\kappa_\nu) \equiv e_\nu(-1)^{\nu-1}\nu! \mod \ell. \tag{4}$$

$$(\nu = 1, 2, \ldots \ell - 1)$$

Übrigens läßt sich hieraus die Hilbertsche Normformel (S. 28]) beweisen. Man findet nämlich leicht:

$$n(\kappa_a) \equiv 1 \mod \ell^2, \quad \text{für} \quad a = 1, 2, \ldots \ell - 2$$
$$n(\kappa_{\ell-1}) \equiv 1 - \ell \mod \ell^2.$$

I, 33 Letzteres ist wegen $\kappa_{\ell-1} = 1 + \ell$ klar. Ersteres folgt aus:

$$\kappa_a = (1 - \lambda^a)^{-r^a(s-1)\ldots(s-r^{a-1})(s-r^{a+1})\ldots(s-r^{\ell-2})}$$

wegen

$$\begin{aligned} n(\kappa_a) &= \kappa_a^{1+s+\cdots+s^{\ell-2}} \equiv \kappa_a^{(s-r)(s-r^2)\ldots(s-r^{\ell-2})} \mod \mathfrak{l}^{\ell+1} \\ &\equiv (1-\lambda^a)^{(s^\ell-1)\,g(s)} \equiv 1 \mod \mathfrak{l}^{\ell+1} \end{aligned}$$

also

$$n(\kappa_a) \equiv 1 \mod \ell^2.$$

Bildet man also in (3) beiderseits die Norm, so wird

$$n(\alpha) \equiv (1-\ell)^{e_{\ell-1}} \equiv 1 - \ell e_{\ell-1} \mod \ell^2$$

d. h. $e_{\ell-1} \equiv \frac{1-n(\alpha)}{\ell}$ mod. ℓ

Andererseits war

$$\ell_{\ell-1}(\alpha) \equiv e_{\ell-1}\,\ell_{\ell-1}(\kappa_{\ell-1}) \equiv e_{\ell-1} \text{ mod. } \ell,$$

da man ja die Behauptung für $\ell_{\ell-1}(\kappa_{\ell-1})$ speziell, wie oben gezeigt, leicht nachrechnen kann. Somit

$$\ell_{\ell-1}(\alpha) \equiv \frac{1-n(\alpha)}{\ell} \text{ mod. } \ell \qquad \text{w. z. b. w.}$$

Setzt man die gefundenen Werte für die $\ell_\nu(\kappa)$ in das Reziprozitätsgesetz S. 29] unten ein, so wird

$$\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)^{-1} = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{-\sum_{a=1}^{\ell-1} a \frac{(-1)^{a-1}\ell_a(\alpha)}{a!}\cdot\frac{(-1)^{\ell-a-1}\ell_{\ell-a}(\beta)}{(\ell-a)!}}$$

Nun ist $\binom{\ell}{a} = \frac{\ell!}{a!\,(\ell-a)!} = \ell \cdot \frac{-1}{a!\,(\ell-a)!} + \cdots$

andererseits $\binom{\ell}{a} = \ell\,\frac{(\ell-1)\ldots\ell-(a-1)}{1\cdot 2\ldots a} = \ell\,\frac{(-1)^{a-1}}{a}$

somit $\frac{a}{a!\,(\ell-a)!} \equiv (-1)^a$ mod. ℓ

I, 34 Damit wird obige Formel

$$\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)^{-1} = \left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\sum_{a=1}^{\ell-1}(-1)^a \ell_a(\alpha)\ell_{\ell-a}(\beta)}$$

(siehe Zahlbericht, S. 413).

Ich berechne nunmehr die zu

$$-\varepsilon = \frac{\lambda^{\ell-1}}{\ell}$$

gehörigen Exponenten. Dazu schreibe ich ε so:

$$\begin{array}{cccccccccccc} (+\varepsilon) & = & \frac{1-\zeta}{1-\zeta} & \cdot & 2\frac{1-\zeta}{1-\zeta 2} & \cdot & 3\frac{1-\zeta}{1-\zeta^3} & \cdots & \cdot(\ell-1)\frac{1-\zeta}{1-\zeta^{\ell-1}} & \cdot & \frac{-1}{(\ell-1)!} \\ & = & \varepsilon_1 & \cdot & \varepsilon_2 & \cdot & \varepsilon_3 & \cdot & \varepsilon_{\ell-1} & \cdot & b \end{array}$$

wo $\varepsilon_1, \ldots, \varepsilon_{\ell-1} \equiv 1 \mod \mathfrak{l}$ und $b \equiv 1 \mod \ell$ ist. Daher wird:

$$\ell_\nu(+\varepsilon) \equiv \ell_\nu(\varepsilon_1) + \ell_\nu(\varepsilon_2) \cdots + \ell_\nu(\varepsilon_{\ell-1}) \text{ mod. } \ell$$
$$\nu = 1, 2, \ldots \ell - 2$$

(Für $\ell - 1$ würde b noch ein Zusatzglied erzeugen, jedoch ist einfach

$$\ell_{\ell-1}(+\varepsilon) \equiv \frac{1 - n(+\varepsilon)}{\ell} \equiv \frac{1 - \frac{\ell^{a-1}}{\ell^{\ell-1}}}{\ell} \equiv 0 \text{ mod. } \ell,$$

sodaß $\nu = \ell - 1$ ausgeschlossen werden kann. Nun gehört zu $\varepsilon_a = a\,\frac{1-\zeta}{1-\zeta^a}$ die Funktion I, 35

$$\varphi_a(e^v) = a\,\frac{1-e^v}{1-e^{av}}$$
$$\log \varphi_a(e^v) = \log \frac{e^v - 1}{v} - \log \frac{e^{av} - 1}{av},$$

wo die Nenner v wegen der Einzelkonvergenz beider Reihen in der Umgebung von $v = 0$ angebracht sind. Ferner ist wie man aus

$$e^{Bv} = \sum_{\nu=0}^{\infty} \frac{B_\nu v^\nu}{\nu!} = \frac{ve^v}{e^v - 1}$$

leicht durch Integration findet:

$$\log \frac{e^v - 1}{v} = \sum_{\nu=1}^{\infty} \frac{B_\nu}{\nu!}\,\frac{v^\nu}{\nu!}$$

Dabei bedeuten die B_ν die Bernoullischen Zahlen:

$$B_1 = \frac{1}{2},\ B_2 = \frac{1}{6},\ B_3 = 0,\ B_4 = -\frac{1}{30}, \cdots$$

Somit wird

$$\log \varphi_a(e^{\nu}) = +\sum_{\nu=1}^{\infty} \left(\frac{B_\nu}{\nu} \frac{v^\nu}{\nu!} - \frac{B_\nu}{\nu} \frac{a^\nu v^\nu}{\nu!} \right)$$

also

$$\ell_\nu(\varepsilon_a) \equiv \frac{B_\nu}{\nu}(1 - a^\nu) \text{ mod. } \ell$$

und

$$\ell_\nu(+\varepsilon) \equiv \frac{B_\nu}{\nu} \sum_{a=1}^{\ell-1} (1 - a^\nu) \text{ mod. } \ell$$

$$\equiv -\frac{B_\nu}{\nu} \text{ mod. } \ell$$

I, 36 weil $\nu \neq \ell - 1$ angenommen wird.

Somit wird nach (4) S. 32] der Exponent e_ν von ε:

$$e_\nu \equiv \frac{(-1)^\nu}{\nu!} \frac{B_\nu}{\nu} \quad \text{mod } \ell \qquad\qquad (\nu = 1, 2, \dots \ell - 2)$$

während $e_{\ell-1}$ nach S. 34] unten Null ist. Also

$$\varepsilon = -\frac{\lambda^{\ell-1}}{\ell} \equiv \kappa_1^{-B_1} \kappa_2^{\frac{B_2}{2\cdot 2!}} \kappa_4^{\frac{B_4}{4\cdot 4!}} \cdots\cdots \kappa_{\ell-3}^{\frac{B_{\ell-3}}{(\ell-3)(\ell-3)!}} \quad \text{mod } \mathfrak{l}^{\ell}$$

da die B_ν für ungerades ν außer B_1 verschwinden.

Wird also

$$f(s) = (s - r)(s - r^2)(s - r^4) \dots (s - r^{\ell-5})$$

gesetzt, so ist

$$\kappa_1^{f(s)} \equiv \kappa_2^{f(s)} \equiv \kappa_4^{f(s)} \equiv \dots \equiv \kappa_{\ell-5}^{f(s)} \equiv 1 \quad \text{mod } \mathfrak{l}^{\ell+1}$$

I, 37 wegen (2) S. 28]. Ferner ist offenbar

$$\kappa_{\ell-3}^{f(s)} \equiv 1 - f(r^{\ell-3})\lambda^{\ell-3} \quad \text{mod } \mathfrak{l}^{\ell-2}$$

Also wird

$$\varepsilon^{f(s)} \equiv 1 - \frac{B_{\ell-3}}{(\ell-3).(\ell-3)!} f(r^{\ell-3})\lambda^{\ell-3} \quad \text{mod } \mathfrak{l}^{\ell-2}.$$

Hiermit ist entsprechend dem Programm von S. 22] eine Einheit gefunden, die für $B_{\ell-3} \not\equiv 0 \bmod. \ell$ den Typus $1 - \iota\lambda^{\ell-3}$ hat $\big(f(r^{\ell-3})$ ist $\not\equiv 0 \bmod. \ell\big)$. *Damit ist der Fermatsche Satz (nur Fall I) für alle Exponenten ℓ bewiesen, für die $B_{\ell-3}$ zu ℓ prim ist.*

Der Ergänzungssatz für $\left(\frac{\lambda}{\alpha}\right)$ erfordert noch die Bestimmung von $\left(\frac{\varepsilon}{\alpha}\right)$. Sei

$$\left(\frac{\varepsilon}{\alpha}\right) = \zeta^c$$

Dann folgt:

$$\left(\frac{\lambda}{\alpha}\right) = \left(\frac{\ell}{\alpha}\right)^{-1}\left(\frac{\varepsilon}{\alpha}\right)^{-1} = \zeta^{e_\ell - c}$$

Um c durch die Exponenten e_i von α in (3) auszudrücken, verwenden wir das allgem. Reziprozitätsgesetz S. 29] unten:

$$\left(\frac{\varepsilon}{\alpha}\right) = \zeta^{-\sum_{a=1}^{\ell-3} a \frac{(-1)^a B_a}{a!\cdot a} e_{\ell-a}} = \zeta^c$$

also

$$c \equiv -\frac{1}{2}\,\frac{n(\alpha)-1}{\ell} - \sum_{\nu=1}^{\frac{\ell-3}{2}} \frac{B_{2\nu}}{(2\nu)!} e_{\ell-2\nu}$$

und somit

$$\left(\frac{\boldsymbol{\lambda}}{\boldsymbol{\alpha}}\right) = \boldsymbol{\zeta}^{e_\ell + \frac{1}{2}\frac{n(\alpha)-1}{\ell} + \sum_{\nu=1}^{\frac{\ell-3}{2}} \frac{B_{2\nu}}{(2\nu)!} e_{\ell-2\nu}}$$

$$\text{für}\quad \alpha = \kappa_1^{e_1}\dots\kappa_\ell^{e_\ell}\,\xi^\ell\ (\mathfrak{l}).$$

1.7 Literatur zum Fermatschen Satz. (23.7.1923)

Hasse collects references for Fermat's Last Theorem.

I, 38

23. VII. 23.

(Nach A. Faik, Taschenbuch f. Math. u. Phys. 1913)

1.) Elementare Diskussionen, ziemlich vollständig bei

Lind, Cantors Abhandl. z. Gesch. d. math. Wiss., Heft $\mathbf{XXVI_2}$, Teubner, 1910

2.) Systematische Darstellung,

Bachmann, Additive Zahlenth., Teubner 1910
S. 433 ff.

3.) *Wieferich*, Journ. f. Mathem. **136**, 1909, S. 293–302

$2^{p-1} \equiv 1 \mod p^2$

4.) *Mirimanoff*, { Journ. f. Math. **128**, 1905, S. 45–68
L'ensign. Math. 1909, 15. November
Journ. f. Math. **139**, 1911, S. 309

Kriterien der Art: $\varphi_i(t) = t - 2^{i-1}t^2 + 3^{i-1}t^3 - \cdots - (p-1)^{i-1}t^{p-1}$

Dann muß $B_{2i}\,\varphi_{p-2i}(t) \equiv 0 \mod p$ sein

$$(t = \tfrac{x}{y}, \tfrac{y}{x}, \ldots)$$

wenn $x^p + y^p + z^p = 0$.

Comptes rendus 1910, 24. Januar:

$$3^{p-1} \equiv 1 \mod p^2$$

5.) *Frobenius*, Berl. Ak. Ber. 1909, 2. Dez. S. 1222 ff. (J. f. Math. **137**)

Einfachere Herleitung von $2^{\mu-1} \equiv 1 \mod p^2$
ebenda 1910, 27. Febr., S. 200 ff.
Einfachere Herleitung der Mirimanoffschen Res[ultate].

I, 39

6.) Zur allgemeinen Orientierung (Ausnahmezahlen, Kummers Leistung):

Hensel, Festschr. zur Feier d. 100. Geb. Ed. Kummers, Teubner 1910.

7.) *Kummer*: Crelle **40**, S. 93–138
Beweis für regulären Kreiskörper.

ebenso: Journ. d. math., **16**, 1851, S. 488

Ferner: Abhandl. d. Kgl. Ak. d. Wiss. Berlin, 1857, S. 43–74
(desgl. Monatsber. S. 275)
weitere Resultate, falls Klassenzahl genau durch p teilbar.

1.8 Die Klassenzahl des Kreiskörpers $\boldsymbol{k(\zeta)}$. (25.7.1923)

Hasse studies the analytic class number formula for the ℓ-th cyclotomic number field following Kummer and Hilbert. (ℓ is an odd prime number.) Eventually he observes that everything can be extended to abelian number fields; for this see the next entry of July 29, 1923.]

I, 40

(nach Kummer, Hilbert) 25. VII. 23.

Grundformel:

$$\zeta_k(s) = \zeta(s)L_0(s)L_1(s)\dots L_{\ell-2}(s)$$

wobei $\zeta_k(s) \longrightarrow$ Kreiskörper
$\zeta(s) \longrightarrow$ rationaler Körper

$L_0(s), \dots L_{\ell-2}(s)$ die $\ell - 1$ L–Reihen nach dem Modul ℓ.
Ferner:

$$\lim_{s=1}(s-1)\zeta_k(s) = hg = h \cdot \frac{R}{w} \cdot \frac{2^{r+1}\pi^{r_2}}{|\sqrt{d}|}$$

Hier

$$\begin{aligned} w &= 2\ell; \quad (\pm 1, \pm\zeta, \pm\zeta^2, \dots \pm \zeta^{\ell-1}) \\ r+1 &= r_1 + r_2 = 0 + \frac{\ell-1}{2} = \frac{\ell-1}{2} = r_2 \\ |d| &= \ell^{\ell-2} \end{aligned}$$

Also wegen $\lim_{s=1}(s-1)\zeta(s) = 1$:

$$h = \frac{2\ell}{R} \frac{\ell^{\frac{\ell-2}{2}}}{(2\pi)^{\frac{\ell-1}{2}}} L_0(1) \dots L_{\ell-1}(1).$$

Bezeichnungen: r primitive Wurzel mod. ℓ
ϱ primitive $(\ell-1)$–te Einheitswurzel

Charaktere:

$$\begin{aligned} \chi_i(n) &= \varrho^{i \operatorname{ind} n} \\ L_i(1) &= \sum_n{}' \frac{\chi_i(n)}{n} \end{aligned}$$

Substitution:

$$\tfrac{1}{n} = \int_0^\infty e^{-nt}dt$$

$$L_i(1) = \int_0^\infty {\sum_n}' \chi_i(n)\, e^{-nt}dt$$

$$n = \nu + k\ell\,, \quad \nu = 1, 2, \dots \ell - 1$$

$$L_1(1) = \int_0^\infty \sum_{\nu=1}^{\ell-1} \chi_i(\nu) \sum_{k=0}^{\infty} e^{-(\nu+k\ell)t}dt$$

I, 41

$$= \int_0^\infty \sum_{\nu=1}^{\ell-1} \chi_i(\nu) e^{-\nu t} \frac{1}{1-e^{-\ell t}}\, dt\,; \quad x = e^{-t}$$

$$= \int_0^1 \frac{\sum_{\nu=1}^{\ell-1} \chi_i(\nu)\, x^\nu}{1-x^\ell}\, \frac{dx}{x} = \int_0^1 \frac{f_i(x)}{1-x^\ell}\, \frac{dx}{x}$$

wenn $f_i(x) = \sum_{\nu=1}^{\ell-1} \chi_i(\nu) x^\nu$ gesetzt wird.
Partialbruchzerlegung:

$$\frac{f_i(x)}{x(1-x^\ell)} = -\frac{1}{\ell} \sum_{k=1}^{\ell-1} \frac{f_i(\zeta^k)}{x-\zeta^k} \qquad \text{(nach elementaren Regeln)}$$

$$f_i(\zeta^\nu) = \sum_{\nu=1}^{\ell-1} \varrho^{i\, \mathrm{ind}\, \nu} \zeta^{k\nu} = \sum_{\nu=0}^{\ell-2} \varrho^{i\nu} \zeta^{kr^\nu} = \big(\varrho^i, \zeta^k\big)$$

(Lagrangesche Resolvente).

$$L_i(1) = -\frac{1}{\ell} \sum_{k=1}^{\ell-1} (\varrho^i, \zeta^k) \int_0^1 \frac{dx}{x-\zeta^k}$$

$$= -\frac{1}{\ell} \sum_{k=1}^{\ell-1} (\varrho^i, \zeta^k) \Big[\log(1-\zeta^k) - \log(-\zeta^k) \Big]$$

wobei beidesmal derselbe Zweig des log zu nehmen ist. *Ich setze den Zweig mit imaginärem Teil zwischen $\pm\pi i$ fest.*

Die Resolventen (ϱ^i, ζ^k) genügen folgendem Gesetz:

$$(\varrho^i, \zeta^{rk}) = \varrho^{-i}(\varrho^i, \zeta^k) \qquad \text{(Ableitung elementar)}$$

I, 42 Wird also über r^a statt k summiert, so wird:

$$\begin{aligned} L_i(1) &= -\frac{1}{\ell}\sum_{a=0}^{\ell-2}(\varrho^i, \zeta^{r^a})\Big[\log(1-\zeta^{r^a}) - \log(-\zeta^{r^a})\Big] \\ &= -\frac{1}{\ell}(\varrho^i, \zeta)\sum_{a=0}^{\ell-2}(\varrho^{-ia}\Big[\log(1-\zeta^{r^a}) - \log(-\zeta^{r^a})\Big] \end{aligned}$$

Die Diskussion muß notwendig die beiden Fälle eines ungeraden und geraden i von hier an trennen.

1.) *i ungerade*

Dann ist $\varrho^{-i(a+\frac{\ell-1}{2})} = -\varrho^{-ia}$
also

$$\begin{aligned} L_i(1) = -\frac{1}{\ell}(\varrho^i, \zeta)\sum_{a=0}^{\frac{\ell-3}{2}}\varrho^{-ia}\Big[&\big\{\log(1-\zeta^{r^a}) - \log(1-\zeta^{-r^a})\big\} \\ &- \big\{\log(-\zeta^{r^a}) - \log(-\zeta^{-r^a})\big\}\Big] \end{aligned}$$

da ja $\zeta^{r^{a+\frac{\ell-1}{2}}} = \zeta^{-r^a}$ ist.

Die reellen Teile der beiden in [ ] stehenden Differenzen { }, { } sind beidesmal 0, da die Argumente der Logarithmen paarweise konjugiert komplex sind. Die imaginären Teile der *einzelnen* Logarithmen sind stets eindeutig durch die Forderung $-\pi i \ldots + \pi i$ bestimmt. Der Wert von { } ist ferner beidesmal das doppelte des imaginären Teils des ersten Gliedes von { } (konjugiert komplexe Zahlen). Bezeichnet nun g_a den kleinsten positiven Rest von r^a, so lehrt eine elementare Diskussion (am besten geometrisch), daß

$$\Im\big(\log(1-\zeta^{r^a})\big) = -\left(\frac{\pi}{2} - \frac{\pi g_a}{\ell}\right) i = \Im_1$$

ist, in welchen „Quadranten“ auch $\frac{2\pi r^a}{\ell}$ fallen mag. Ebenso

$$\Im\big(\log(-\zeta^{r^a})\big) = -\left(\pi - \frac{2\pi g_a}{\ell}\right) i = \Im_2$$

Also I, 43

$$\begin{aligned} [\ ] &= 2(\Im_1 - \Im_2) \\ &= \frac{\pi i}{\ell}(\ell - 2g_a) \end{aligned}$$

und daher

$$L_1(1) = -\frac{1}{\ell}(\varrho^i, \zeta) \sum_{a=0}^{\frac{\ell-3}{2}} \varrho^{-ia} \frac{\pi i}{\ell}(\ell - 2g_a)$$

$$\begin{aligned} &= -\frac{\pi i}{\ell^2}(\varrho^i, \zeta) \left\{ -\sum_{a=0}^{\frac{\ell-3}{2}} g_a \varrho^{-ia} + \sum_{a=0}^{\frac{\ell-3}{2}} (\ell - g_a)\varrho^{-ia} \right\} \\ &= +\frac{\pi i}{\ell^2}(\varrho^i, \zeta) \left\{ \sum_{a=0}^{\frac{\ell-3}{2}} g_a\, \varrho^{-ia} + \sum_{a=\frac{\ell-1}{2}}^{\ell-2} (\ell - g_{a-\frac{\ell-1}{2}})\varrho^{-ia} \right\} \\ &= +\frac{\pi i}{\ell^2}(\varrho^i, \zeta) \sum_{a=0}^{\ell-2} g_a \varrho^{-ia}, \qquad \left\{ \begin{array}{ll} \text{da} & g_a + g_{a-\frac{\ell-1}{2}} = \ell \\ \text{wegen} & r^a \equiv -r^{a-\frac{\ell-1}{2}} \mod \ell \end{array} \right\} \end{aligned}$$

also schließlich:

$$\boxed{L_i(1) = \frac{\pi i}{\ell^2}(\varrho^i, \zeta) \sum_{n=1}^{\ell-1} n \varrho^{-i\,\mathrm{ind}.n} \qquad \text{für ungerades } i.}$$

Abgebrochen, da sich die Klassenzahl nach derselben Methode ganz allgemein für jeden absolut Abelschen Körper bestimmen läßt.

1.9 Die Klassenzahl absolut Abelscher Körper. (29.7.1923)

In Part a) Hasse starts investigating the functional equation of L-series in the abelian case. As a tool he considers the polynomials $\sum \chi(\nu)x^\nu$ *for Dirichlet characters* χ*, these are nowadays called Fekete polynomials. In fact they have their origins in the evaluation of Dirichlet's class number formula. Part b) is dedicated to an investigation of discriminants via functional equations of zeta functions and L-series, an idea going back to Hecke. Finally, Part c) gives the application to the class number formula for real and complex abelian extensions of the rationals. Special cases are quadratic fields and cyclotomic fields. Hasse reports that he follows Artin in this treatment. We see that this entry is another outcome of Artin's visit to Hasse in July 1923. We note that earlier, on July 9, 1923 Artin had briefly informed Hasse about his newly found L-functions for Galois characters* [FR08]. *In the treatment of those new functions he had to fall back on the classical Dirichlet L-functions (on that occasion he conjectured his new reciprocity law). The functional equation for those implied the validity of the functional equation for Artin's new L-functions and thus their behavior on the complex plane. It appears that Artin had explained Hasse the details and thereby also the proof of the functional equation for the classical Dirichlet L-functions. In Hasse's class field report* [Has26a] *he presents Parts a) and b) essentially as given here, but without giving a detailed proof of the functional equation of L-series. Later, Hasse has given a systematic and detailed treatment of the arithmetic structure of the class number formulas in his book* [Has52].

I, 44

(Nach Dr. Artin) 29. VII. 23.

a.) Die Funktionalgleichung der L–Reihen.

Sei χ ein eigentlicher Charakter nach dem Führer f. Dann betrachten wir die Summen:

$$\Phi(x, \chi) = \sum_{\nu=1}^{f} \chi(\nu) x^\nu$$

Satz 1. *Für* $(\mu, f) > 1$ *ist* $\Phi(\varepsilon^\mu, \chi) = 0$*, wenn* $\varepsilon = e^{\frac{2\pi i}{f}}$ *die primitive* f*–te Einheitswurzel ist.*

Beweis: Sei $(\mu, f) = a > 1$ und $f = af_0$. Ist dann r eine beliebige, zu f prime Zahl $\equiv 1 \mod f_0$, so ist

$$\varepsilon^{\nu\mu r} = \varepsilon^{\nu\mu}$$

da

$$\varepsilon^{\nu\mu(r-1)} = \varepsilon^{\nu\mu k f_0}$$

wegen $\mu = a\mu_0$ einen durch $af_0 = f$ teilbaren Exponenten hat, also 1 ist. Daher ist

$$\Phi(\varepsilon^\mu, \chi) = \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\nu\mu} = \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\nu\mu r}$$

Nun durchläuft νr mit ν ein primes Restsystem mod f, während für $(\nu, f) > 1$ $\big($wo $\chi(\nu) = 0\big)$ auch $(\nu r, f) > 1$ ist und umgekehrt. Daher ist

$$\begin{aligned} \Phi(\varepsilon^\mu, \chi) &= \chi(r^{-1}) \sum_{\nu=1}^{f} \chi(\nu r)\varepsilon^{\nu\mu r} = \chi(r^{-1}) \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\nu\mu} \\ &= \chi(r^{-1})\Phi(\varepsilon^\mu, \chi). \end{aligned}$$

Wenn also $\Phi(\varepsilon^\mu, \chi) \neq 0$, so folgte: I, 45

$$\chi(r) = 1$$

für jedes zu f prime $r \equiv 1 \mod f_0$, also

$$\chi(\nu_1) = \chi(\nu_2)$$

für irgendzwei $\nu_1 \equiv \nu_2 \mod f_0$, die prim zu f sind. Dann wäre aber χ schon mod f_0 definierbar, also uneigentlich. Also ist $\Phi(\varepsilon^\mu, \chi) = 0$, w. z. b. w.

Satz 2. *Für $(\mu, f) = 1$ ist $\Phi(\varepsilon^\mu, \chi) = \overline{\chi}(\mu)\Phi(\varepsilon, \chi)$, wo $\overline{\chi}$ den konjugiert komplexen Charakter bezeichnet. Wegen Satz 1 gilt also diese Formel für jedes μ.*

Beweis: Ist $(\mu, f) = 1$, so ist

$$\begin{aligned} \Phi(\varepsilon^\mu, \chi) &= \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\nu\mu} = \chi(\mu^{-1}) \sum_{\nu=1}^{f} \chi(\nu\mu)\varepsilon^{\nu\mu} \\ &= \overline{\chi}(\mu) \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\nu} = \overline{\chi}(\mu)\Phi(\varepsilon, \chi) \end{aligned}$$

nach einer ebensolchen Überlegung, wie a. v. S.] unten.

Wir betrachten nun die Summen:

$$\mathsf{S}_\kappa = \sum_{\nu=1}^{f} \chi(\nu) \sin\left(\frac{s}{s} + \frac{2\kappa\nu}{f}\right)\pi \,.$$

Aus

$$\sin\left(\frac{s}{2} + \frac{2\kappa\nu}{f}\right)\pi = \frac{1}{2i}\left[e^{\frac{i\pi s}{s} + \frac{2i\pi\kappa\nu}{f}} - e^{-\frac{i\pi s}{2} - \frac{2i\pi\kappa\nu}{f}}\right]$$

folgt:

$$\begin{aligned} \mathsf{S}_\kappa \quad &= \quad \frac{1}{2i} e^{\frac{i\pi s}{2}} \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\kappa\nu} - \frac{1}{2i} e^{-\frac{i\pi s}{2}} \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{-\kappa\nu} \\ &= \quad \frac{1}{2i} e^{\frac{i\pi s}{2}} \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\kappa\nu} - \frac{1}{2i} \varepsilon^{-\frac{i\pi s}{2}} \chi(-1) \sum_{\nu=1}^{f} \chi(\nu)\varepsilon^{\kappa\nu} \\ &= \quad \frac{1}{2i}\left[e^{\frac{i\pi s}{2}} - \chi(-1) e^{-\frac{i\pi s}{2}}\right] \Phi(\varepsilon^\kappa, \chi) \end{aligned}$$

I, 46

Je nachdem nun $\chi(-1) = +1$ oder -1 ist, wird nach Satz 2:

$$\begin{aligned} \mathsf{S}_\kappa \quad &= \sin\frac{\pi s}{2} \overline{\chi}(\kappa)\Phi(\varepsilon, \chi) \\ \text{bzw.} \quad \mathsf{S}_\kappa \quad &= \frac{1}{i} \cos\frac{\pi s}{2} \overline{\chi}(\kappa)\Phi(\varepsilon, \chi). \end{aligned}$$

Es gilt also:

$$(1) \qquad \sum_{\nu=1}^{f} \chi(\nu) \sin\left(\frac{s}{2} + \frac{2\kappa\nu}{f}\right)\pi = \begin{cases} \overline{\chi}(\kappa)\Phi(\varepsilon, \chi) \sin\frac{\pi s}{2} & \text{für} \quad \chi(-1) = +1 \\ \overline{\chi}(\kappa)\frac{\Phi(\varepsilon,\chi)}{i} \cos\frac{\pi s}{2} & \text{für} \quad \chi(-1) = -1 \end{cases}$$

Die entwickelten Formeln finden Anwendung bei Herleitung der Funktionalgleichung der L–Reihen im rationalen Körper nach dem Führer f. Ist χ ein eigentlicher Charakter mod. f so ist die zu ihm gehörige L–Reihe definiert durch

$$(2) \qquad L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{\nu=1}^{f} \chi(\nu) \sum_{m=0}^{\infty} \frac{1}{(\nu + mf)^s} = \sum_{\nu=1}^{f} \chi(\nu)\zeta_\nu(s) \,,$$

wobei

$$\zeta_\nu(s) = \sum_{m=0}^{\infty} \frac{1}{(\nu + mf)^s} \qquad \text{für} \quad \nu = 1, 2, \dots f$$

gesetzt ist.

Vermöge $\frac{\Gamma(s)}{n^s} = \int\limits_0^\infty e^{-nt} t^{s-1} dt\,;\ (\sigma > 1) \quad (\Re(s) = \sigma)$.

wird

$$\begin{aligned}\Gamma(s)\zeta_\nu(s) &= \sum_{m=0}^{\infty} \int\limits_0^\infty e^{-(\nu+mf)f} t^{s-1}\, dt \\ &= \int\limits_0^\infty e^{-\nu t} t^{s-1} \sum_{m=0}^{\infty} e^{-mft}\, dt\end{aligned}$$

da wegen der gleichmäßigen Konvergenz der $\sum_{m=0}^{\infty}$ mit vorstehendem Faktor für $t \geqq 0$ Summation und Integration vertauscht werden darf. Es wird somit I, 47

$$\Gamma(s)\zeta_\nu(s) = \int\limits_0^\infty \frac{e^{-\nu t}}{1 - e^{-ft}}\, t^{s-1} dt\,; \qquad (\sigma > 1)$$

Dabei ist $t^{s-1} = e^{(s-1)\lg t}$ mit einer solchen ein– für allemal getroffenen Normierung von $\lg t$, daß $\lg t$ für reelle t reell ist. Zur Verwandlung in ein Schleifenintegral denkt man die t Ebene längs der positiv reellen Achse aufgeschnitten und den imaginären Teil von $\lg t$ zwischen 0 und 2π festgesetzt. Dann wird das Schleifenintegral

$$\begin{aligned}\psi_\nu(s) &= \int\limits_{\subset\!\rightleftarrows} \frac{e^{-\nu t}}{1 - e^{-ft}}\, t^{s-1} dt \\ &= \int\limits_\infty^0 \frac{e^{-\nu t}}{1 - e^{-ft}}\, e^{(s-1)[\log t + 2\pi i]} dt + \int\limits_0^\infty \frac{e^{-\nu t}}{1 - e^{-ft}}\, e^{(s-1)\lg t} dt\,,\end{aligned}$$

da das Integral um einen kleinen, den Nullpunkt umschließenden Kreis für $\sigma > 1$ gegen Null konvergiert (Zähler $O\big(|t|^{\sigma-1}\big)$, Nenner $O\big(|t|\big)$, also Integrand $O\big(|t|^{\sigma-2}\big)$ sodaß

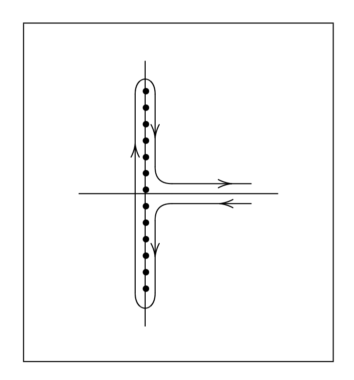
$$\int\limits_{\circlearrowright} O\big(|t|^{\sigma-2}\big) = O\big(|t|^{\sigma-1}\big) = o(1) \qquad \text{für} \quad \sigma > 1) :$$

Somit wird

$$\psi_\nu(s) = \left(1 - e^{2\pi i s}\right) \int_0^\infty \frac{e^{-\nu t}}{1 - e^{-ft}}\, t^{s-1} dt$$

$$\psi_\nu(s) = -2ie^{\pi i s} \sin \pi s\, \zeta_\nu(s) \Gamma(s) \tag{3}$$

Da $\psi_\nu(s)$ durch seine Schleifenintegraldarstellung als ganze Funktion erkannt wird, wird hierdurch auch $\zeta_\nu(s)$ über die ganze s–Ebene fortgesetzt. $\zeta_\nu(s)$ ist nur dort singulär, wo $\sin \pi s\, \Gamma(s) = 0$, also einzig und allein für $s = 1$, da für $s =$ I, 48 $2, 3, \ldots$ $\psi_\nu(s)$ ebenfalls von der 1. Ordnung verschwindet. Das Schleifenintegral $\psi_\nu(s)$ wird nun durch Deformation des Weges ausgewertet, indem die Schleife um den Nullpunkt nach oben und unten über alle Pole 1. Ordnung $t = \pm\frac{2\pi i k}{f}$ auf der imaginären Achse hinweggezogen wird.

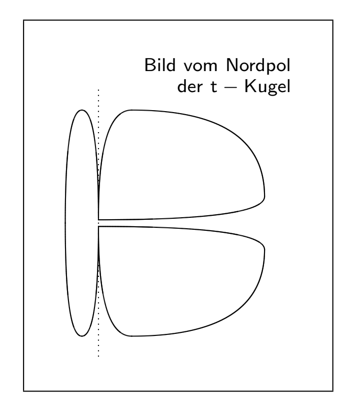


Daraus ist ersichtlich, daß das Schleifenintegral gleich wird dem deformierten Schleifenintegral + Summe der Residuen $\times 2\pi i$ der überschrittenen Pole (+ Zeichen wegen des Umlaufsinnes).

Dieser Prozeß darf längs der imaginären Achse bis zum Punkte $\pm i\infty$ fortgesetzt werden, denn auf den Parallelen im Abstand ± 1 zur imaginären Achse wird der Integrand

$$\leqq \frac{e^{\pm\nu}}{1 - e^{\pm f}} (1 + i\mathsf{T})^{\sigma-1} = O\left(|\mathsf{T}|^{\sigma-1}\right)$$

strebt also gleichmäßig zu Null, wenn $\mathsf{T} = \Im(t) \to \pm\infty$, und für $\sigma < 0$ so, daß das Integral längs dieser Geraden konvergiert.



Da der deformierte Weg auf seiner anderen Seite keine Singularitäten des Integranden mehr umschließt, ist das deformierte Integral Null, sodaß nur noch die Summe der Residuen $\times 2\pi i$ übrig bleibt. Nun ist das Residuum von $\frac{1}{1-e^{-ft}}$ im Pol $t = \frac{2\pi ik}{f}$ gleich

I, 49

$$\lim_{t=\frac{2\pi ik}{f}} \frac{t - \frac{2\pi ik}{f}}{1 - e^{-ft}} = \frac{1}{f}$$

Somit wird das Residuum des Integranden $\frac{e^{-\nu t}}{1-e^{-ft}}\, t^{s-1}$

$$r_k = \frac{1}{f} e^{-\frac{2\pi ik\nu}{f}} \left(\frac{2\pi ik}{f}\right)^{s-1} = \frac{1}{f^s} \varepsilon^{-k\nu} (2\pi i)^{s-1} k^{s-1}$$

also für $\sigma < 0$:

$$\begin{aligned}
\psi_\nu(s) &= \sum_{k=-\infty}^{+\infty}{}' (2\pi i)^s \frac{1}{f^s} \varepsilon^{-k\nu} k^{s-1} \\
&= \left(\frac{2\pi i}{f}\right)^s \sum_{k=1}^{\infty} (\varepsilon^{-k\nu} + e^{\pi i(s-1)} \varepsilon^{k\nu}) k^{s-1} \\
&= \left(\frac{2\pi}{f}\right)^s e^{\frac{\pi is}{2}} \sum_{k=1}^{\infty} (\varepsilon^{-k\nu} - e^{\pi is} \varepsilon^{k\nu}) k^{s-1} \\
&= \left(\frac{2\pi}{f}\right)^s e^{\frac{\pi is}{2}} e^{\frac{\pi is}{2}} \sum_{k=1}^{\infty} -2i \sin\left(\frac{s}{2} + \frac{2k\nu}{f}\right) \pi \cdot k^{s-1} \\
&= -\left(\frac{2\pi}{f}\right)^s e^{\pi is} 2i \sum_{\mu=1}^{f} \sin\left(\frac{s}{2} + \frac{2\nu\mu}{f}\right) \pi \sum_{m=0}^{\infty} (\mu + mf)^{s-1} \\
&= -2i \left(\frac{2\pi}{f}\right)^s e^{\pi is} \sum_{\mu=1}^{f} \sin\left(\frac{s}{2} + \frac{2\nu\mu}{f}\right) \pi \cdot \zeta_\mu(1-s)
\end{aligned}$$

Aus (3) folgt also, zunächst für $\sigma < 0$, also wegen der Fortsetzbarkeit von $\zeta_\nu(s)$ allgemein für alle s:

$$(4) \qquad \sin\pi s\,\Gamma(s)\,\zeta_\nu(s) = \left(\frac{2\pi}{f}\right)^s \cdot \sum_{\mu=1}^{f} \sin\left(\frac{s}{2} + \frac{2\nu\mu}{f}\right)\pi \cdot \zeta_\mu(1-s)$$

Diese Funktionalgleichung wird nunmehr zur Aufstellung einer Funktionalgleichung für die $L(s,\chi)$ verwendet. Nach (2),(4) ist:

$$\sin\pi s\,\Gamma(s)\,L(s,\chi) = \left(\frac{2\pi}{f}\right)^s \sum_{\mu=1}^{f} \zeta_\mu(1-s) \sum_{\nu=1}^{f} \chi(\nu)\sin\left(\frac{s}{2} + \frac{2\nu\mu}{f}\right)\pi$$

I, 50 Es wird somit nach (1):

$$\sin\pi s\,\Gamma(s)L(s,\chi) = \left(\frac{2\pi}{f}\right)^s \sum_{\mu=1}^{f} \zeta_\mu(1-s)\overline{\chi}(\mu)$$

$$\begin{cases} \sin\frac{\pi s}{2} \cdot \Phi(\varepsilon,\chi) & \text{für} \quad \chi(-1) = +1 \\ \cos\frac{\pi s}{2} \cdot \frac{\Phi(\varepsilon,\chi)}{i} & \quad '' \quad \chi(-1) = -1 \end{cases}$$

d. h. nach leichter Umrechnung, wenn von jetzt an die beiden Fälle $\chi(-1) = +1$ bezw. -1 stets durch A.) B.) unterschieden werden:

$$(5\,\text{A.}) \qquad L(1-s,\overline{\chi}) = \frac{2\cos\frac{\pi s}{2}\,\Gamma(s)}{\left(\frac{2\pi}{f}\right)^s\,\Phi(\varepsilon,\chi)}\,L(s,\chi)\,,$$

$$(5\,\text{B.}) \qquad L(1-s,\overline{\chi}) = i\,\frac{2\sin\frac{\pi s}{2}\,\Gamma(s)}{\left(\frac{2\pi}{f}\right)^s\,\Phi(\varepsilon,\chi)}\,L(s,\chi)\,.$$

Aus (5 A.), (5 B.) geht durch die Substitution $s : 1-s$ unter Berücksichtigung von

$$\Gamma(s)\,\Gamma(1-s) = \frac{\pi}{\sin\pi s}$$

und

$$\begin{aligned} \cos\frac{\pi(1-s)}{2} &= \sin\frac{\pi s}{2} \\ \sin\frac{\pi(1-s)}{2} &= \cos\frac{\pi s}{2} \end{aligned}$$

hervor:

$$L(1-s,\overline{\chi}) = \frac{2\cos\frac{\pi s}{2}\,\Gamma(s)\Phi(\varepsilon,\overline{\chi})}{f\left(\frac{2\pi}{f}\right)^s}\,L(s,\chi)\,, \tag{6 A.}$$

$$L(1-s,\overline{\chi}) = -i\,\frac{2\sin\frac{\pi s}{2}\,\Gamma(s)\Phi(\varepsilon,\overline{\chi})}{f\left(\frac{2\pi}{f}\right)^s}\,L(s,\chi)\,. \tag{6 B.}$$

Durch Vergleich von (5.) und (6.) ergibt sich sofort

$$\left.\begin{array}{lrcl} (7\,\text{A.}) & \Phi(\varepsilon,\overline{\chi})\Phi(\varepsilon,\chi) & = & f \\ (7\,\text{B.}) & \Phi(\varepsilon,\overline{\chi})\Phi(\varepsilon,\chi) & = & -f \end{array}\right\}\ \text{also}\ \ \Phi(\varepsilon,\chi)\Phi(\varepsilon,\overline{\chi}) = \chi(-1)f$$

Nun ist das konjugiert komplexe I, 51

$$\overline{\Phi(\varepsilon,\chi)} = \Phi(\varepsilon^{-1},\overline{\chi}) = \overline{\chi}(-1)\,\Phi(\varepsilon,\overline{\chi}) = \chi(-1)\,\Phi(\varepsilon,\overline{\chi})$$

nach Satz 2, also

$$\Phi(\varepsilon,\chi)\cdot\overline{\Phi(\varepsilon,\chi)} = f$$

und somit

$$\bigl|\Phi(\varepsilon,\chi)\bigr| = \sqrt{f} \tag{8}$$

Es sei nun im folgenden $\sqrt{x}$ stets positiv, wenn x positiv, positiv imaginär, wenn x negativ. Wird dann

$$\eta(\chi) = \frac{\Phi(\varepsilon,\chi)}{\sqrt{\chi(-1)f}} \tag{8a.}$$

gesetzt, so ist wegen (8) zunächst

$$\bigl|\eta(\chi)\bigr| = 1\,, \tag{9}$$

ferner

$$\begin{aligned} \overline{\eta(\chi)} &= \frac{\chi(-1)\Phi(\varepsilon,\overline{\chi})}{\chi(-1)\sqrt{\chi(-1)f}} = \frac{\Phi(\varepsilon,\overline{\chi})}{\sqrt{\chi(-1)f}} \\ \eta(\overline{\chi}) &= \frac{\Phi(\varepsilon,\overline{\chi})}{\sqrt{\chi(-1)f}}\,, \end{aligned}$$

da im ersten Falle das konjugierte zu $\sqrt{\chi(-1)f}$ für $\chi(-1) = +1$ ungeändert, für $\chi(-1) = -1$ entgegengesetzt gleich wird. Es gilt somit:

$$\overline{\eta(\chi)} = \eta(\overline{\chi}) \tag{10}$$

Schreibt man also (6 A.), (6 B.) in der Form:

$$L(1-s,\chi) = \frac{2}{(2\pi)^s} \left\{ \begin{matrix} \cos\frac{\pi s}{2} \\ \sin\frac{\pi s}{2} \end{matrix} \right\} \Gamma(s)\, f^{s-\frac{1}{2}} \omega(\chi)\, L(s,\overline{\chi}),$$

I, 52 (worin nach früher Festsetzung $f^{-\frac{1}{2}} = \frac{1}{\sqrt{f}}$ positiv ist), sodaß also:

$$\left.\begin{array}{lccc} \text{A.)} & \omega(\chi) & = & \dfrac{\Phi(\varepsilon,\chi)}{\sqrt{f}} \\ \text{B.)} & \omega(\chi) & = & \dfrac{\Phi(\varepsilon,\chi)}{i\sqrt{f}} = \dfrac{\Phi(\varepsilon,\chi)}{\sqrt{-f}} \end{array}\right\} = \frac{\Phi(\varepsilon,\chi)}{\sqrt{\chi(-1)f}} = \eta(\chi)$$

ist, so erhält man die Funktionalgleichung:

$$\boxed{\begin{array}{ll} (11.\,\text{A.}) & L(1-s,\chi) = \dfrac{2}{(2\pi)^s}\,\eta(\chi) f^{s-\frac{1}{2}} \cos\dfrac{\pi s}{2}\,\Gamma(s)L(s,\chi) \\ (11.\,\text{B.}) & L(1-s,\chi) = \dfrac{2}{(2\pi)^s}\,\eta(\chi) f^{s-\frac{1}{2}} \sin\dfrac{\pi s}{2}\,\Gamma(s)L(s,\overline{\chi}). \end{array}}$$

Darin hat $\eta(x)$ nach (9) den absoluten Betrag 1 und genügt der Relation (10), die nunmehr unmittelbar in Evidenz setzt, daß (11.) bei $s : 1-s$ und $\chi : \overline{\chi}$ in sich übergeht, denn es folgt ja aus (10),(11.)

$$\frac{1}{\eta(\chi)} = \overline{\eta(\chi)} = \eta(\overline{\chi}).$$

Die Funktionalgleichung (11.) gestattet natürlich den analytischen Charakter der L–Reihen zu diskutieren. Man findet wegen $L(s,\overline{\chi}) \neq 0$ für $\sigma > 0$, $\Gamma(s) \neq 0$, daß die L–Reihen A.) für $s = 0, -2, -4, \ldots$ die L–Reihen B.) für $s = -1, -3, -5, \ldots$ verschwinden, und zwar von erster Ordnung. Bekanntlich ist außer für den Hauptcharakter, wo die ζ–Funktion vorliegt, $L(1,\chi)$ endlich $\neq 0$. Die sämtlichen L–Reihen außer $\zeta(s)$ sind also ganze transzendente Funktionen, die außer den vorgegebenen trivialen Nullstellen nur solche im Streifen $0 < \sigma < 1$

I, 53 haben (Man kann beweisen: $L(s,\chi) \neq 0$ für $\sigma = 1$).

b.) Die Diskriminante Abelscher Körper.

Aus dem Vergleich der gefundenen Funktionalgleichung der L–Reihen mit der Heckeschen Funktionalgleichung der ζ–Funktion des betr. algebraischen Körpers ergibt sich eine Reihe wichtiger Tatsachen.

Zunächst gilt die Grundformel:

$$\zeta_K(s) = \prod_{\chi} L(s,\chi) \tag{12}$$

wobei K irgendeinen absolut Abelschen Körper bedeutet, und χ alle Charaktere *der* Restklassengruppe im rationalen Grundkörper durchläuft, nach der K Klassenkörper ist, und zwar jedesmal die eigentlichen Charaktere.

Es sei nun $\mathfrak{m}$ der Führer dieser Restklassengruppe, also K Unterkörper des zur Gruppe „$\equiv 1 \mod \mathfrak{m}$, total positiv“ gehörigen Kreiskörpers der $\mathfrak{m}$–ten Einheitswurzeln ($\mathfrak{m}$ ist als Führer natürlich stets entweder ungerade oder durch 4 teilbar). Ferner sei n der Grad von K, und es mögen existieren:

$$\begin{array}{llcccc} n_1 & \text{Charaktere} & : & \chi(-1) & = & +1 \\ n_2 & \quad\text{"} & : & \chi(-1) & = & -1 \end{array}$$

also

$$n_1 + n_2 = n$$

Aus (12), (11.) ergibt sich dann:

$$\zeta_K(1-s) = \left(\frac{2}{(2\pi)^s}\right)^n \prod_{\chi} \eta(\chi) \prod_{\chi} \big(f(\chi)\big)^{s-\frac{1}{2}} \left(\cos\frac{\pi s}{2}\right)^{n_1} \left(\sin\frac{\pi s}{2}\right)^{n_2} \big(\Gamma(s)\big)^n \zeta_K(s)$$

Die Heckesche Funktionalgleichung für $\zeta_K(s)$ lautet (Landau, Analytische Idealtheorie, S. 75): I, 54

$$\zeta_K(1-s) = \left(\frac{2}{(2\pi)^s}\right)^n |\Delta|^{s-\frac{1}{2}} \left(\cos\frac{\pi s}{2}\right)^{r_1+r_2} \left(\sin\frac{\pi s}{2}\right)^{r_2} \big(\Gamma(s)\big)^n \zeta_K(s)$$

Daraus folgt durch Vergleichung sukzessive:

$$\begin{cases} n_1 = r_1 + r_2\,, \\ n_2 = r_2\,, \end{cases} \tag{13}$$

$$(14) \qquad \prod_{\chi} f(\chi) = |\Delta|\,,$$

$$(15) \qquad \prod_{\chi} \eta(\chi) = 1\,.$$

Aus (13) folgt, da K Galoissch ist, wenn A.) und B.) jetzt den Fall eines reellen bzw. imaginären K unterscheiden:

$$(16\,\mathsf{A.}) \quad \begin{cases} n_1 = n \\ n_2 = 0 \end{cases} \qquad\qquad (16\,\mathsf{B.}) \quad \begin{cases} n_1 = \frac{n}{2} \\ n_2 = \frac{n}{2} \end{cases}$$

wo ferner allgemein sgn. $\Delta = (-1)^{r_2}$ ist (aus der Darstellung als Differenzenprodukt leicht zu entnehmen), folgt aus (14):

$$(17\,\mathsf{A.}) \quad \Delta = \prod_{\chi} f(\chi) \qquad\qquad (17\,\mathsf{B.}) \quad \Delta = (-1)^{\frac{n}{2}} \prod_{\chi} f(\chi)\,.$$

Aus (15.) schließlich folgt nach (8a.):

$$(18) \qquad \prod_{\chi} \Phi(\varepsilon, \chi) = i^{n_2} \sqrt{|\Delta|}$$

Ist speziell χ ein reeller Charakter vom Führer f, so gehört zu ihm ein quadratischer Unterkörper, durch die Forderung $\chi(\nu) = 1$ wird nämlich eine bestimmte Untergruppe vom Führer f definiert (Definition des Führers eines Charakters), die wegen $\chi(\nu^2) = \big(\chi(\nu)\big)^2 = 1$ vom Index 2 ist. Zu dieser Untergruppe als Hauptklasse, ihrer Nebengruppe als Nebenklasse gehört ein quadratischer Klassenkörper. Die Charaktere der neuen Klasseneinteilung sind $\chi'_0(\nu) = 1$ (Hauptcharakter) $\chi'_1(\nu) = +1$ oder -1, je nachdem $\chi(\nu) = +1$ oder -1, d. h. $\chi'_1(\nu) = \chi(\nu)$. Die Diskriminante d des so entstehenden quadratischen Körpers ist nach (14)

I, 55

$$|d| = f,$$

weil der Hauptcharakter den Führer 1, der andere mit χ identische den Führer f hat. Das Vorzeichen von d ergibt sich, indem die vorstehenden Betrachtungen auf unseren quadr. Körper angewandt werden:

Ist $\chi(-1) = +1$, so ist $n_1 = 2$, $n_2 = 0$, also der Körper reell:

$$d = f\,.$$

Ist dagegen $\chi(-1) = -1$, so ist $n_1 = 1$, $n_2 = 1$, also der Körper imaginär und

$$d = -f\,,$$

stets also

$$d = \chi(-1)f\,.$$

Daher folgt, weil für den Hauptcharakter $f = 1$, also $\Phi(\varepsilon, \chi) = 1$, $\eta(\chi_0) = 1$ ist, und somit nach (14) für den anderen Charakter I, 56

$$1 = \eta(\chi) = \frac{\Phi(\varepsilon, \chi)}{\sqrt{\chi(-1)f}} = \frac{\Phi(\varepsilon, \chi)}{\sqrt{d}}$$

ist,

$$\Phi(\varepsilon, \chi) = \sqrt{d}$$

womit das Vorzeichen der Gaussschen Summen für reelle Charaktere bestimmt ist.

c.) Die Klassenzahl Abelscher Körper.

Für die Bestimmung der Klassenzahl muß das Residuum von $\zeta_K(s)$ für $s = 1$ bestimmt werden. Es ist nach (12):

$$\lim_{s=1}(s-1)\zeta_K(s) = \lim_{s=1}(s-1)\prod_{\chi} L(s, \chi)\,,$$

d. h. da zum Hauptcharakter die Funktion $\zeta(s)$ mit dem Residuum 1 gehört:

$$\lim_{s=1}(s-1)\zeta_K(s) = {\prod_{\chi}}' L(1, \chi)\,,$$

wo das Produkt über alle Nichthauptcharaktere zu erstrecken ist. Nun ist für einen Nichthauptcharakter χ vom Führer f:

$$L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} = \sum_{\nu=1}^{f} \chi(\nu) \sum_{m=0}^{\infty} \frac{1}{\nu + mf}\ ,$$

oder mittels

$$\frac{1}{n} = \int_0^1 x^{n-1} dx :$$

$$\begin{aligned} L(1,\chi) &= \sum_{\nu=1}^{f} \chi(\nu) \sum_{m=0}^{\infty} \int_0^1 x^{\nu+mf-1} dx \\ &= \int_0^1 \sum_{\nu=1}^{f} x^{\nu-1} \chi(\nu) \frac{1}{1-x^f}\, dx\,, \end{aligned}$$

I, 57 da wegen der gleichmäßigen Konvergenz von

$$\sum_{\nu=1}^{f} x^{\nu-1} \chi(\nu) \sum_{m=0}^{\infty} x^{mf}$$

für $0 \leqq x \leqq 1$, (es ist $\sum_{\nu=1}^{f} \chi(\nu) = 0$), gliedweise integriert werden darf. Also wird (siehe S. 44]):

$$L(1,\chi) = -\int_0^1 \frac{\Phi(x,\chi)}{x^f - 1} \frac{dx}{x}$$

Die Zerlegung des Integranden in Partialbrüche nach der für „verschiedene Nennerfaktoren" gültigen Identität:

$$\frac{g(x)}{f(x)} = \frac{g(x)}{(x-\alpha_1)\dots(x-\alpha_n)} = \sum_{\nu=1}^{n} \frac{g(\alpha_\nu)}{f'(\alpha_\nu)} \frac{1}{x-\alpha_\nu}$$

(wenn $g(x)$ von niedrigerem Grad als $f(x)$)

ergibt hier:

$$\frac{\Phi(x,\chi)}{x(x^f-1)} = \frac{\Phi(x,\chi)}{x(x-1)(x-\varepsilon)\cdots(x-\varepsilon^{f-1})} = \sum_{\nu=0}^{f-1} \frac{\Phi(\varepsilon^\nu,\chi)}{f} \frac{1}{x-\varepsilon^\nu}$$

Da $\Phi(0,\chi) = 0$ ist. Das Glied mit $\nu = 0$ wird wegen $\Phi(1,\chi) = \sum_{\nu=1}^{f} \chi(\nu) = 0$ ebenfalls 0. Daher gilt:

$$L(1,\chi) = -\int_0^1 \sum_{\nu=1}^{f-1} \frac{\Phi(\varepsilon^\nu,\chi)}{f} \frac{dx}{x-\varepsilon^\nu}$$

oder nach Satz 2:

$$L(1,\chi) = -\frac{\Phi(\varepsilon,\chi)}{f}\sum_{\nu=1}^{f-1}\overline{\chi}(\nu)\int\limits_0^1 \frac{dx}{x-\varepsilon^\nu}\ .$$

Nun setzen wir

$$x = \varepsilon^\nu(1-y), \quad \text{also} \quad x-\varepsilon^\nu = -\varepsilon^\nu y$$
$$dx = -\varepsilon^\nu\, dy$$
$$x = 0 \ \rightarrow \ y = 1$$
$$x = 1 \ \rightarrow \ y = 1-\varepsilon^{-\nu}$$

Dann wird: I, 58

$$\int\limits_0^1 \frac{dx}{x-\varepsilon^\nu} = \int\limits_1^{1-\varepsilon^{-\nu}} \frac{dy}{y} = \log(1-\varepsilon^{-\nu})$$

wo der log hier, wie im folgenden stets den Hauptwert bezeichnet, denn das ursprünglich geradlinig zu erstreckende Integral $\int\limits_0^1$ geht durch die lineare Transformation wieder in ein geradliniges über, sodaß der Nullpunkt in $\int\limits_1^{1-\varepsilon^{-\nu}}$ nicht umlaufen wird. (Der Hauptwert ist mit imaginärem Teil zwischen $\pm\pi i$ zu nehmen). Es wird daher

$$L(1,\chi) = -\frac{\Phi(\varepsilon,\chi)}{f}\sum_{\nu=1}^{f-1}\overline{\chi}(\nu)\log(1-\varepsilon^{-\nu})$$

$$\lim_{s=1}(s-1)\zeta_K(s) = \prod{}' L(1,\chi) = (-1)^{n-1}\frac{i^{n_2}}{\sqrt{|\Delta|}}\prod_\chi{}'\sum_{\nu=1}^{f-1}\overline{\chi}(\nu)\log(1-\varepsilon^{-\nu})$$

weil für den Hauptcharakter $\Phi(\varepsilon,\chi) = 1$, also (18) auch hier anwendbar ist. Da $\overline{\chi}$ mit χ alle Charaktere durchläuft, darf auch

$$\lim_{s=1}(s-1)\zeta_K(s) = (-1)^{n-1}\frac{i^{n_2}}{\sqrt{|\Delta|}}\prod_\chi{}'\sum_{\nu=1}^{f-1}\chi(\nu)\log(1-\varepsilon^{-\nu})$$

geschrieben werden.

Nun sind wieder die beiden Fälle

A) $\chi(-1) = +1$ B) $\chi(-1) = -1$

zu trennen.

A.) $\chi(-1) = +1$.

Dann wird

$$\mathsf{S} = \sum_{\nu=1}^{f-1} \chi(\nu) \log(1 - \varepsilon^{-\nu})$$

auch zu

$$\mathsf{S} = \sum_{\nu=1}^{f-1} \chi(\nu) \log(1 - \varepsilon^{\nu})$$

I, 59 also, da $(1-\varepsilon^{-\nu})$ und $(1-\varepsilon^{\nu})$ konjugiert komplex sind, und daher $\log(1-\varepsilon^{\nu}) + \log(1-\varepsilon^{-\nu}) = \log(1-\varepsilon^{\nu})(1-\varepsilon^{-\nu})$ *in Hauptwerten* gesetzt werden muß:

$$\begin{aligned} \mathsf{S} &= \frac{1}{2}\sum_{\nu=1}^{f-1} \chi(\nu) \log(1-\varepsilon^{\nu})(1-\varepsilon^{-\nu}) \\ &= \sum_{\nu=1}^{f-1} \chi(\nu) \log\sqrt{(1-\varepsilon^{\nu})(1-\varepsilon^{-\nu})}, \end{aligned}$$

wo die Wurzel *positiv* zu nehmen ist.

Sei nun $\zeta = e^{\frac{2\pi i}{\mathfrak{m}}}$, $\mathfrak{m} = af$, $\varepsilon = \zeta^a$; dann ist

$$(1-\varepsilon^{\nu}) = \prod_{k=0}^{a-1} \left(1 - \zeta^{\nu+kf}\right)$$

da ζ^0, ζ^f, ... $\zeta^{(a-1)f}$ die a–ten Einheitswurzeln sind; damit wird

$$\log\sqrt{(1-\varepsilon^{\nu})(1-\varepsilon^{-\nu})} = \sum_{k=0}^{a-1} \log\sqrt{(1-\zeta^{\nu+kf})(1-\zeta^{-\nu-kf})}$$

wenn geeignet zusammengefaßt wird. Da nun

$$\chi(\nu) = \chi(\nu + kf)$$

ist, darf

$$\mathsf{S} = \sum_{k=0}^{a-1}\sum_{\nu=1}^{f-1} \chi(\nu+kf)\log\sqrt{(1-\zeta^{\nu+kf})(1-\zeta^{-\nu-kf})}$$

geschrieben werden, und da schließlich $\chi(\nu+kf)=0$ für $\nu=0$, auch

$$\mathsf{S} = \sum_{\nu=1}^{\mathfrak{m}-1} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}\,.$$

Da schließlich noch $\chi(\mathfrak{m}-\nu)=\chi(-\nu)=\chi(\nu)$ ist dies:

$$\mathsf{S} = 2\sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})} \tag{19}$$

Da für gerades $\mathfrak{m}$ zu dem „mittleren“ Glied mit $\nu=\frac{\mathfrak{m}}{2}$ ein $\chi(\nu)=\chi\left(\frac{\mathfrak{m}}{2}\right)=0$ gehört. $\frac{\mathfrak{m}}{2}$ hat nämlich mit $\mathfrak{m}$ alle Primfaktoren bis auf 2 gemeinsam, und letzteren nur dann nicht, wenn $\mathfrak{m}\equiv 2 \mod 4$, was als Führer ein Restklassengruppe für $\mathfrak{m}$ nicht eintreten kann. Daher hat $\frac{\mathfrak{m}}{2}$ mit jedem Führer einen Teiler gemein, so daß $\chi\left(\frac{\mathfrak{m}}{2}\right)=0$, wenn χ nicht der Hauptcharakter. I, 60

B.) $\chi(-1)=-1$.

Dann wird

$$\mathsf{S} = \sum_{\nu=1}^{f-1}\chi(\nu)\log(1-\varepsilon^{-\nu})$$

auch zu

$$\mathsf{S} = -\sum_{\nu=1}^{f-1}\chi(\nu)\log(1-\varepsilon^{\nu})\,,$$

also

$$\mathsf{S} = \frac{1}{2}\sum_{\nu=1}^{f-1}\chi(\nu)\Big(\log(1-\varepsilon^{-\nu})-\log(1-\varepsilon^{\nu})\Big).$$

Nun ist

$$\begin{aligned}
1-\varepsilon^{-\nu} &= 1-e^{-\frac{2\pi i\nu}{f}} \\
&= e^{-\frac{\pi i\nu}{f}}\left(e^{\frac{\pi i\nu}{f}}-e^{-\frac{\pi i\nu}{f}}\right) = 2i\sin\frac{\pi\nu}{f}e^{-\frac{\pi i\nu}{f}} \\
1-\varepsilon^{-\nu} &= 2e^{-\frac{\pi i\nu}{f}+\frac{\pi i}{2}}\sin\frac{\pi\nu}{f}\,, \\
1-\varepsilon^{\nu} &= 2e^{\frac{\pi i\nu}{f}-\frac{\pi i}{2}}\sin\frac{\pi\nu}{f}
\end{aligned}$$

also, da $(1-\varepsilon^{-\nu})$ und $(1-\varepsilon^{\nu})$ gleichen Betrag haben, die Logarithmendifferenz gleich der Differenz der (in obigen Formeln zwischen $\pm\pi i$ gelegenen) Amplituden. Daher ist:

$$\mathsf{S} = \frac{1}{2}\sum_{\nu=1}^{f-1}\chi(\nu)\left[-\frac{2\pi i\nu}{f}+\pi i\right] = -\frac{\pi i}{f}\sum_{\nu=1}^{f-1}\nu\chi(\nu)$$

Ferner wird, wenn $af=\mathfrak{m}$ ist

$$\sum_{\nu=1}^{\mathfrak{m}-1}\nu\chi(\nu) = a\sum_{\nu=1}^{f-1}\nu\chi(\nu),$$

weil für einen Teil der $\sum\limits_{1}^{\mathfrak{m}-1}$:

$$\begin{aligned}\sum_{\nu=kf+1}^{(k+1)f-1}\nu\chi(\nu) = \sum_{\nu=1}^{f-1}(kf+\nu)\chi(\nu) &= \sum_{\nu=1}^{f-1}\nu\chi(\nu)+kf\sum_{\nu=1}^{f-1}\chi(\nu)\\ &= \sum_{\nu=1}^{f-1}\nu\chi(\nu)\quad \text{ist,}\end{aligned}$$

I, 61 und die durch f teilbaren ν ein $\chi(\nu)=0$ haben.

Daher wird

$$\mathsf{S} = -\frac{\pi i}{\mathfrak{m}}\sum_{\nu=1}^{\mathfrak{m}-1}\nu\chi(\nu)\,. \tag{20}$$

Aus (19) und (20) folgt nun sofort nach obiger Formel:

$$\begin{aligned}\lim_{s=1}(s-1)\zeta_K(s) = &(-1)^{n-1}\frac{i^{n_2}}{\sqrt{|\Delta|}}\prod_{\chi(-1)=+1}{}' \; 2\sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}}\chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}\\ &(-1)^{n_2}\prod_{\chi(-1)=-1}\frac{\pi i}{\mathfrak{m}}\sum_{\nu=1}^{\mathfrak{m}-1}\nu\chi(\nu)\,.\end{aligned}$$

A. **Reeller Körper**.

Dann ist $\left\{\begin{array}{l} n_1 = n \\ n_2 = 0 \end{array}\right\}$, sodaß der zweite Faktor ganz wegfällt, und es wird

$$\lim_{s=1}(s-1)\zeta_K(s) = (-1)^{n-1}\frac{2^{n-1}}{\sqrt{|\Delta|}}\prod_{\chi}{}' \sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}$$

andererseits

$$h = \frac{w}{\mathsf{R}}\frac{\sqrt{|\Delta|}}{2^n}\lim_{s=1}(s-1)\zeta_K(s)$$

also:

$$\begin{aligned} h &= \frac{w}{\mathsf{R}}(-1)^{n-1}\frac{1}{2}\prod_{\chi}{}' \sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})} \\ &= (-1)^{n-1}\frac{\prod'_{\chi}\sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}, \quad \text{da } w = 2 \end{aligned}$$

I, 62

B. **Imaginärer Körper**.

Hier ist $n_1 = n_2 = \frac{n}{2}$, ferner

$$\begin{aligned} &\lim_{s=1}(s-1)\zeta_K(s) \\ = \ &(-1)^{n-1}\frac{i^{\frac{n}{2}}}{\sqrt{|\Delta|}}\prod_{\chi(-1)=+1}{}' 2\sum_{\nu=1}^{\leqq\frac{\mathfrak{m}-1}{2}} \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})} \\ &(-1)^{\frac{n}{2}}\left(\frac{\pi i}{\mathfrak{m}}\right)^{\frac{n}{2}}\prod_{\chi(-1)=-1}\sum_{\nu=1}^{\mathfrak{m}-1}\nu\chi(\nu)\,. \\ = \ &(-1)^{n-1}\frac{\pi^{\frac{n}{2}}2^{\frac{n}{2}-1}}{\sqrt{|\Delta|}\,\mathfrak{m}^{\frac{n}{2}}}\prod_{\chi(-1)=+1}{}' \chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})} \\ &\prod_{\chi(-1)=-1}\sum_{\nu=1}^{\mathfrak{m}-1}\nu\chi(\nu) \end{aligned}$$

und

$$h = \frac{w}{\mathsf{R}}\frac{\sqrt{|\Delta|}}{2^{\frac{n}{2}}\pi^{\frac{n}{2}}}\lim_{s=1}(s-1)\zeta_K(s)$$

d. h. wegen n gerade:

$$h = -\frac{w}{\mathsf{R}} \frac{1}{2} \frac{1}{\mathfrak{m}^{\frac{n}{2}}} \prod_{\chi(-1)=+1}' \cdots \prod_{\chi(-1)=-1} \cdots$$

Wird nun in der Determinante R für jede der eingehenden $\frac{n}{2} - 1$ Grundeinheiten anstatt des doppelten nur der einfache Logarithmus genommen, und dies wieder als Regulator R bezeichnet, so wird

$$h = -\frac{w \prod_{\chi(-1)=-1} \sum_{\nu=1}^{\mathfrak{m}-1} \nu\chi(\nu)}{(2\mathfrak{m})^{\frac{n}{2}}} \cdot \frac{\prod'_{\chi(-1)=+1} \sum_{\nu=1}^{\leqq \frac{\mathfrak{m}-1}{2}} \chi(\nu) \log \sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}$$

I, 63 Es gelten also folgende beiden Endformeln:

A. **Reeller Körper**.

$$h = (-1)^{n-1} \frac{\prod'_{\chi} \sum_{\nu=1}^{\leqq \frac{\mathfrak{m}-1}{2}} \chi(\nu) \log \sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}$$

B. **Imaginärer Körper**.

$$h = -\frac{w \prod_{\chi(-1)=-1} \sum_{\nu=1}^{\mathfrak{m}-1} \nu\chi(\nu)}{(2\mathfrak{m})^{\frac{n}{2}}} \cdot \frac{\prod'_{\chi(-1)=+1} \sum_{\nu=1}^{\leqq \frac{\mathfrak{m}-1}{2}} \chi(\nu) \log \sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}} .$$

Dabei bedeuten:

$\mathfrak{m}$	Führer der Klassengruppe, nach der K Klassenkörper
n	Grad von K
w	Anzahl der Einheitswurzeln in K
ζ	$= e^{\frac{2\pi i}{\mathfrak{m}}}$
χ	Die Charaktere der Restklassengruppe mod $\mathfrak{m}$, für die K Klassenkörper, und zwar die *eigentlichen*
$\prod\limits_{\chi(-1)=\pm 1}'$	Produkt über alle Charaktere der angegebenen Art, ausgenommen den Hauptcharakter.
R	Die Determinante $$\mathsf{R} = \Big\| \,\big| \log \lvert\varepsilon_i^{(k)}\rvert \big|\, \Big\| \qquad \begin{array}{ll} i & = 1, 2, \ldots r \\ k & = 1, 2, \ldots r \end{array}$$ dem Betrage nach, wo $\varepsilon_i^{(k)}$ die $r = r_1 + r_2 - 1$ Grundeinheiten mit ihren (nicht konjugiert komplexen konjugierten)

Für I, 64 imaginär quadratische Körper ist natürlich der zweite Faktor gleich 1 zu setzen, da dann nach (13) nur ein Charakter mit $\chi(-1) = +1$, der Hauptcharakter existiert und $\mathsf{R} = 1$ zu setzen ist.

d.) Anwendung auf quadratische Körper.

Jeder quadratische Körper hat nur zwei Charaktere, den Hauptcharakter und einen davon verschiedenen χ. Ist f der Führer von χ, so ist die Diskriminante

$$d = \chi(-1)\, f$$

(s. S. 55]). Durch Diskussion aller Restklassengruppen vom Index 2 erhält man hieraus leicht die bekannten Sätze über Diskriminanten quadratischer Körper.

A. **Reell–quadratischer Körper**.

Dann ist $\chi(-1) = +1$, $d = f$. Für die Klassenzahl ergibt sich nach obiger Formel

$$h = -\frac{\sum_{\nu=1}^{\leq \frac{\mathfrak{m}-1}{2}} \chi(\nu) \log \sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\big| \log \lvert\varepsilon\rvert \big|}$$

wenn ε die Grundeinheit ist. Der Führer $\mathfrak{m}$ der Restklassengruppe ist natürlich $\mathfrak{m} = f = d$, weil nur ein Charakter vom Führer f außer dem Hauptcharakter existiert. Dieser Charakter selbst wird durch das Jacobi–Symbol $\left(\frac{d}{n}\right)$ gegeben, denn dieses ist einerseits nur von der Restklasse abhängig der n mod d. angehört, wie man auf Grund der „Diskriminanteneigenschaft“ von d leicht mittels I, 65

des Reziprozitätsgesetzes beweist, andererseits definiert es durch $\left(\frac{d}{n}\right) = 1$ eine Untergruppe, die wegen $\left(\frac{d}{n^2}\right) = 1$ den Index 2 hat. Auch ohne Benutzung des Reziprozitätsgesetzes und der Diskriminanteneigenschaft von d folgt dies einfach daraus, daß der quadratische Körper mit der Diskriminante d das Zerlegungsgesetz:

$$\text{Wenn} \quad \left(\tfrac{d}{p}\right) = +1, \quad p = \mathfrak{p}_1\mathfrak{p}_2$$

$$\text{"} \quad \left(\tfrac{d}{p}\right) = -1, \quad p = \mathfrak{p}$$

hat, also die Klassengruppe nach der er Klassenkörper ist durch die an ihre Primzahlen zu stellende Forderung $\chi(p) = \left(\frac{d}{p}\right) = 1$ eindeutig charakterisiert ist. Daraus folgt, daß diese Klassengruppe durch

$$\chi(n) = \left(\frac{d}{n}\right) = 1$$

definiert ist, und da d nach obigem Führer dieser Klassengruppe, daß $\left(\frac{d}{n}\right)$ nur von der Restklasse von $n \mod d$ abhängt, d. h. im Wesentlichen das quadratische Reziprozitätsgesetz.

Um die Klassenzahlformel auf die übliche Gestalt zu bringen, nehmen wir anstatt der nur halb erstreckten Zählersummen wieder die volle (s. S. 59] unten)

I, 66

$$\begin{aligned}
&\frac{1}{2}\sum_{\nu=1}^{d-1}\left(\frac{d}{n}\right)\log\sqrt{(1-e^{\frac{2\pi i\nu}{d}})(1-e^{-\frac{2\pi i\nu}{d}})} \\
= \; &\frac{1}{2}\sum_{\nu=1}^{d-1}\left(\frac{d}{n}\right)\log\sqrt{(e^{-\frac{\pi i\nu}{d}}-e^{\frac{\pi i\nu}{d}})(e^{\frac{\pi i\nu}{d}}-e^{-\frac{\pi i\nu}{d}})} \\
= \; &\frac{1}{2}\sum_{\nu=1}^{d-1}\left(\frac{d}{n}\right)\log\sqrt{4\sin^2\frac{\pi\nu}{d}} \\
= \; &\frac{1}{2}\sum_{\nu=1}^{d-1}\left(\frac{d}{n}\right)\log^2\sin\frac{\pi\nu}{d}
\end{aligned}$$

Bezeichnet man also, wie üblich, die „Reste“ nach d mit a, die „Nichtreste“ mit b, sodaß $\left(\frac{d}{a}\right) = 1$, $\left(\frac{d}{b}\right) = -1$ gilt, so wird

$$\boldsymbol{h = \frac{1}{2\log\varepsilon}\cdot\log\frac{\prod_b \sin\frac{\pi b}{d}}{\prod_a \sin\frac{\pi a}{d}}}\ ,$$

wobei ε die positive Grundeinheit > 1 bezeichnet.

B. **Imaginär Quadratischer Körper**.

Dann ist $\chi(-1) = -1$, $d = -f$. Es gelten entsprechende Betrachtungen, wie unter A.) Der Führer der Klassengruppe ist jetzt $|d|$, ihr Charakter $\chi(n) = \left(\frac{d}{n}\right)$. Somit ergibt sich aus obiger Formel

$$h = -\frac{w}{2|d|}\sum_{\nu=1}^{|d|-1}\left(\frac{d}{\nu}\right)\nu$$

$$\boldsymbol{h = \frac{w}{2d}\left\{\sum_{a} a - \sum_{b} b\right\}}$$

I, 67

e.) Anwendung auf den Kreiskörper.

Der Kreiskörper der m–ten Einheitswurzeln gehört zur Restklassengruppe $\equiv 1 \mod m$, total positiv; wenn der triviale Fall $m \equiv 2 \mod 4$, (wo m durch $\frac{m}{2}$ ersetzt werden muß, um Führer der Gruppe zu sein), ausgeschlossen wird, ist m Führer dieser Gruppe. Diese Restklassengruppe hat als „Idealgruppe“ im Grundkörper den Index $\varphi(m)$, da einerseits $2\varphi(m)$ Repräsentanten (mit Vorzeichenbedingung) mod m existieren, andererseits je 2 Repräsentanten $\pm\nu$ als Ideal betrachtet übereinstimmen. Man erhält somit folgende Klassenzahlformel:

$$h = -\frac{w\prod_{\chi(-1)=-1}\sum\limits_{\nu=1}^{m-1}\nu\chi(\nu)}{(2m)^{\frac{1}{2}\varphi(m)}} \cdot \frac{\prod'_{\chi(-1)=+1}\sum\limits_{\nu=1}^{\leqq\frac{m-1}{2}}\chi(\nu)\log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}$$

Die Anzahl w der Einheitswurzeln ist m oder $2m$ je nachdem m gerade oder ungerade ist. (Siehe Hilbert, Zahlbericht, S. 376).

Ist $m = \ell$ eine ungerade Primzahl, so gestattet dieser Ausdruck noch einige Vereinfachungen. Zunächst ist dann $w = 2\ell$. Die Charaktere χ sind ferner sämtlich eigentliche Charaktere des Führers ℓ und stellen sich durch eine primitive $(\ell-1)$ te Einheitswurzel ϱ so dar:

$$\chi_k(\nu) = \varrho^{ki}, \quad \text{wenn} \quad \nu \equiv r^i \mod \ell$$

und r primitive Wurzel mod. ℓ. Wegen $-1 \equiv r^{\frac{\ell-1}{2}}$ mod. ℓ ist $\chi_k(-1) = \varrho^{k\frac{\ell-1}{2}} = (-1)^k$. Es wird somit

I, 68

$$h = -\frac{\prod\limits_{k=1,3,\ldots\,\ell-2} \sum_{\nu=1}^{\ell-1} \nu \varrho^{k \operatorname{ind} \nu}}{(2\ell)^{\frac{\ell-3}{2}}} \cdot \frac{\prod\limits_{k=2,4,\ldots\,\ell-3} \sum_{\nu=1}^{\frac{\ell-1}{2}} \chi_k(\nu) \log \sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}$$

Der Zähler des zweiten Faktors läßt sich ebenfalls in einer R entsprechenden Determinantenform schreiben.

Ist nämlich

$$\Delta = |x_{\mathsf{PQ}^{-1}}|$$

die Determinante der regulären Gruppenmatrix einer Abelschen Gruppe mit den Charakteren χ, so geht Δ durch Addition der mit $\frac{\chi(\mathsf{P})}{\chi(\mathsf{P}_n)}$ multiplizierten Zeilen zur letzten Zeile über in eine Determinante mit der letzten Zeile

$$\overline{\chi}(\mathsf{P}_n) \sum_{\mathsf{P}} \chi(\mathsf{P})\, x_{\mathsf{PQ}^{-1}}\,; \quad (\mathsf{Q} = \mathsf{Q}_1, \mathsf{Q}_2, \ldots\, \mathsf{Q}_n)$$

Δ ist somit teilbar durch die sämtlichen Linearformen

$$\sum_{\mathsf{P}} \chi(\mathsf{P}) x_{\mathsf{P}}$$

denn die letzte Zeile läßt sich auch schreiben:

$$\overline{\chi}(\mathsf{P}_n)\chi(\mathsf{Q}) \sum_{\mathsf{P}} \chi(\mathsf{P}) x_{\mathsf{P}}$$

Da diese Linearformen alle verschieden sind und ihre Anzahl mit dem Grad der Gruppe und der Anzahl der Charaktere übereinstimmt, muß bis auf eine Konstante

I, 69

$$\Delta = |x_{\mathsf{PQ}^{-1}}| = c \prod_{\chi} \sum_{\mathsf{P}} \chi(\mathsf{P}) x_{\mathsf{P}}$$

sein. Durch $x_{\mathsf{E}} = 1$, $x_{\mathsf{P}} = 0$ folgt $c = 1$, also:

$$\Delta = |x_{\mathsf{PQ}^{-1}}| = \prod_{\chi} \sum_{\mathsf{P}} \chi(\mathsf{P})\, x_{\mathsf{P}}$$

Nun bilden die Charaktere $\chi_0, \chi_2, \ldots\, \chi_{\ell-3}$ offensichtlich eine Untergruppe der Gruppe aller Charaktere, und ihr korrespondiert in der Restklassengruppe mod.

ℓ die Untergruppe „$\equiv \pm 1$ mod. ℓ", sodaß die genannten Charaktere Charaktere für die Nebengruppen dieser Untergruppe sind. Denn die Gesamtheit aller Elemente, für die alle jene Charaktere 1 sind, d. h. die Hauptklasse für die ihnen zugeordnete Klassengruppe ist „$\equiv \pm 1$ mod. ℓ". Ein Repräsentantensystem für diese Klassen sind gerade die Zahlen 1, 2, … $\frac{\ell-1}{2}$. I, 70

Als Repräsentanten können auch genommen werden die Restklassen:

$$r^0, r^1, \ldots, r^{\frac{\ell-3}{2}}$$

die untereinander inkongruent und mit $\pm$ Zeichen versehen wegen $r^{\frac{\ell-1}{2}} \equiv -1$ mod. ℓ alle Restklassen erschöpfen. Setzt man dann:

$$x_{r^\nu} = \log\sqrt{(1-\zeta^{r^\nu})(1-\zeta^{-r^\nu})} \qquad \nu = 0, 1, \ldots \frac{\ell-3}{2}$$

so wird das zu bestimmende Produkt:

$$\prod_{k=2,4,\ldots\,\ell-3} \chi_k(r^\nu)x_{r^\nu}$$

Anstattdessen bestimmen wir zunächst:

$$\prod_{k=0,2,\ldots\,\ell-3} \chi_k(r^\nu)x_{r^\nu}$$

was nach obiger Formel gleich:

$$\Delta = |x_{r^{\nu-\mu}}| = |x_{r^{-\nu+\mu}}|$$

wird. Unter Berücksichtigung von $x_{r^{-a}} = x_{r^{\frac{\ell-1}{2}-a}}$ wird diese Determinante folgende zyklische Determinante: I, 71

$$\Delta = \begin{pmatrix} x_{r^0} & x_{r^1} & \ldots & x_{r^{\frac{\ell-3}{2}}} \\ x_{r^{\frac{\ell-3}{2}}} & x_{r^0} & \ldots & x_{r^{\frac{\ell-5}{2}}} \\ & & & \\ x_{r^1} & x_{r^2} & \ldots & x_{r^0} \end{pmatrix}$$

Addiert man hier alle Zeilen zur ersten, so tritt der Faktor $\sum\limits_{\nu=0}^{\frac{\ell-3}{2}} x_{r^\nu}$ vor und es

bleibt:

$$\Delta = \sum_{\nu=0}^{\frac{\ell-3}{2}} x_{r^\nu} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ x_{r^{\frac{\ell-3}{2}}} & x_{r^0} & x_{r^1} & \dots & x_{r^{\frac{\ell-5}{2}}} \\ x_{r^{\frac{\ell-5}{2}}} & x_{r^{\frac{\ell-3}{2}}} & x_{r^0} & \dots & x_{r^{\frac{\ell-3}{2}}} \\ \vdots & \vdots & \vdots & & \vdots \\ x_{r^1} & x_{r^2} & x_{r^3} & \dots & x_{r^0} \end{vmatrix}$$

Die restliche Determinante ist gerade unser zu bestimmendes Produkt $\prod\limits_{k=2,4,\dots\,\ell-3}$.
Durch Subtraktion jeder Zeile von der folgenden geht sie, wenn

$$x_{r^\nu} - x_{r^{\nu-1}} = y_{r^\nu}$$

gesetzt wird, wegen $x_{r^\nu} = x_{r^{\nu'}}$, wenn

$$\nu \equiv \nu' \mod \frac{\ell-1}{2} ,$$

über in

$$\prod_{k=2,4,\dots\,\ell-3} = \begin{vmatrix} y_{r^0} & y_{r^1} & \dots & y_{r^{\frac{\ell-5}{2}}} \\ y_{r^{\frac{\ell-3}{2}}} & y_{r^0} & \dots & y_{r^{\frac{\ell-7}{2}}} \\ & & & \\ y_{r^2} & y_{r^3} & \dots & y_{r^0} \end{vmatrix}$$

I, 72 Den Größen y_{r^ν} entsprechen offenbar folgende Kreiskörpergrößen:

$$y_{r^\nu} = \log \sqrt{\frac{(1-\zeta^{r^\nu})(1-\zeta^{-r^\nu})}{(1-\zeta^{r^{\nu-1}})(1-\zeta^{-r^{\nu-1}})}} = \log \varepsilon_\nu$$

Die ε_ν sind *Einheiten*. Natürlich ist $\varepsilon_\nu = \varepsilon_{\nu'}$, wenn $\nu \equiv \nu' \mod \frac{\ell-1}{2}$, sodaß schließlich die fragliche Determinante übergeht in:

$$\mathsf{P} = \begin{vmatrix} \log\varepsilon_0 & \log\varepsilon_1 & \dots & \log\varepsilon_{\frac{\ell-5}{2}} \\ \log\varepsilon_{\frac{\ell-3}{2}} & \log\varepsilon_{\frac{\ell-1}{2}} & \dots & \log\varepsilon_{\frac{\ell-8}{2}} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{vmatrix}$$

wo jede Zeile die vorhergehende zyklisch fortsetzt. (Hilbert, Zahlbericht S. 377 gibt eine etwas andere Anordnung, die durch Zeilen– und Spaltenvertauschungen hervorgeht).

Es gilt also folgender Satz:

Satz 1. *Die Klassenzahl des Kreiskörpers der ℓ–ten Einheitswurzeln wird gegeben durch den Ausdruck:*

$$h = \frac{\prod\limits_{k=1,3,\dots \ell-2} \sum_{\nu=1}^{\ell-1} \nu \varrho^{k \operatorname{ind} \nu}}{(2\ell)^{\frac{\ell-3}{2}}} \cdot \left(-\frac{\mathsf{P}}{\mathsf{R}}\right)$$

Darin bedeutet ϱ eine primitive $(\ell-1)$ te Einheitswurzel, der ind. *bezieht sich auf eine primitive Wurzel r* mod. ℓ. R *ist der aus den einfachen (nicht mit 2 multiplizierten) Logarithmen der Grundeinheiten gebildete Regulator und* P *die Determinante* I, 73

$$\mathsf{P} = \begin{vmatrix} \log \varepsilon_0 & \log \varepsilon_1 & \dots & \log \varepsilon_{\frac{\ell-5}{2}} \\ \log \varepsilon_{\frac{\ell-3}{2}} & \log \varepsilon_{\frac{\ell-1}{2}} & \dots & \log \varepsilon_{\ell-4} \\ \log \varepsilon_{\ell-3} & \log \varepsilon_{\ell-2} & \dots & \log \varepsilon_{\frac{3\ell-11}{2}} \\ \dots & \dots & \dots & \dots \end{vmatrix}$$

wobei allgemein log *den reellen Wert und ε_ν die Einheit*

$$\varepsilon_\nu = \sqrt{\frac{(1-\zeta^{r^\nu})(1-\zeta^{-r^\nu})}{(1-\zeta^{r^{\nu-1}})(1-\zeta^{-r^{\nu-1}})}}$$

bedeutet (mit positiv genommener Wurzel, die in k_ζ stets aufgeht).

Um die Bedeutung des zweiten Klassenzahlfaktors als Klassenzahlfaktors $-\frac{\mathsf{P}}{\mathsf{R}}$ als Klassenzahl des reellen, durch $\zeta + \zeta^{-1}$ bestimmten Unterkörpers zu beweisen, beweisen wir zunächst:

Satz 2. *Jedes System von Grundeinheiten des reellen Unterkörpers $k(\zeta+\zeta^{-1})$ ist auch System von Grundeinheiten von $k(\zeta)$ und umgekehrt kann ein beliebiges System von Grundeinheiten von $k(\zeta)$ durch Anbringung passender Einheitswurzeln stets in ein solches für $k(\zeta+\zeta^{-1})$ verwandelt werden. Insbesondere sind also die Regulatoren beider Körper gleich, wenn wie immer von den Faktoren 2, die für $k(\zeta)$ eigentlich hinzutreten, abgesehen wird.* I, 74

Beweis: Die Anzahlen der Grundeinheiten sind in beiden Körpern gleich, nämlich $\frac{\ell-3}{2}$.

Sei ferner $\varepsilon(\zeta)$ eine beliebige Einheit aus $k(\zeta)$, dann ist $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ eine Einheit, deren sämtliche konjugierte den Betrag 1 haben, also Einheitswurzeln aus $k(\zeta)$,

d. h.

$$\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} = \pm\zeta^{2g}$$

Dann ist $\eta(\zeta) = \varepsilon(\zeta)\cdot\zeta^{-g}$ eine Einheit aus $k(\zeta)$ mit der Eigenschaft

$$\eta(\zeta) = \pm\eta(\zeta^{-1}).$$

Es muß aber das + Zeichen gelten; sonst wäre nämlich $\eta(\zeta)$ rein imaginär, ferner $\eta^2 = \vartheta$ Einheit aus $k(\zeta+\zeta^{-1})$, da sie bei $(\zeta : \zeta^{-1})$ in sich übergeht. $k(\zeta)$ würde also von $k(\zeta+\zeta^{-1})$ aus durch $\eta = \sqrt{\vartheta}$ definiert. Die Relativdifferente der Zahl η wäre dann $2\sqrt{\vartheta} = 2\eta$ also prim zu ℓ, somit auch die Relativdifferente und Relativdiskriminante von $k(\zeta)$ nach $k(\zeta+\zeta^{-1})$, da ja nur ein Primideal in beiden Körpern als Teiler von ℓ vorkommt. Das ist aber unmöglich, weil bekanntlich gilt:

$$\begin{array}{lll} & \text{In } k(\zeta+\zeta^{-1}): & \ell = \mathfrak{l}_1^{\frac{\ell-1}{2}} \\ & \text{In } k(\zeta) & \ell = \mathfrak{l}^{\ell-1} \\ \text{Also:} & \text{In } k(\zeta) & \mathfrak{l}_1 = \mathfrak{l}^2. \end{array}$$

I, 75 Es ist somit

$$\eta(\zeta) = \eta(\zeta^{-1})$$

d. h. die Einheit $\varepsilon(\zeta)\zeta^{-g} = \eta(\zeta)$ gehört zu $k(\zeta+\zeta^{-1})$. Auf diese Weise kann jedes System von Grundeinheiten von $k(\zeta)$ durch Multiplikation mit geeigneten Einheitswurzeln in ein System von Einheiten des Unterkörpers verwandelt werden. Diese müssen natürlich *Grundeinheiten* von $k(\zeta+\zeta^{-1})$ sein, da sonst *auch im Oberkörper* $k(\zeta)$ noch ein System niedrigeren Regulators folgen würde. Umgekehrt ist dann natürlich auch *jedes* System von Grundeinheiten von $k(\zeta+\zeta^{-1})$ ein solches für $k(\zeta)$, da nach dem schon Bewiesenen die Regulatoren übereinstimmen, w. z. b. w.

Nach der Grundformel für die Klassenzahl reeller Körper (S. 63]) wird nun die Klassenzahl von $k(\zeta+\zeta^{-1})$:

$$h_1 = (-1)^{\frac{\ell-3}{2}} \frac{\prod'_{\chi} \sum_{\nu=1}^{\frac{\ell-1}{2}} \log\sqrt{(1-\zeta^{\nu})(1-\zeta^{-\nu})}}{\mathsf{R}}$$

wo R den Regulator des Kreiskörpers bedeutet. Die Charaktere, die hier in Frage kommen sind gerade diejenigen, die für die Restklassen ±1 mod. ℓ (die jetzige Hauptklasse im Grundkörper) 1 sind, also genau die mit $\chi(-1) = +1$.

Daher ist

$$h_1 = (-1)^{\frac{\ell-3}{2}} \frac{\mathsf{P}}{\mathsf{R}}$$

wo P die vorhin angegebene Determinante ist. I, 76

Um die Vorzeichen in beiden Klassenzahlformeln richtig (positiv) zu bekommen, muß man also den zweiten Faktor als $(-1)^{\frac{\ell-3}{2}} \frac{\mathsf{P}}{\mathsf{R}}$ und somit den ersten als $(-1)^{\frac{\ell-1}{2}} \frac{\prod \sum}{\cdots}$ schreiben. Es gilt somit

Satz 3. *Die Klassenzahl des Kreiskörpers der ℓ–ten Einheitswurzeln stellt sich mit den Bezeichnungen von Satz 1 als Produkt zweier* positiver *Faktoren in der Form dar*

$$h = (-1)^{\frac{\ell-1}{2}} \frac{\prod_{k=1,3,\ldots\ell-2} \sum_{\nu=1}^{\ell-1} \nu \varrho^{k \operatorname{ind} \nu}}{(2\ell)^{\frac{\ell-3}{2}}} \cdot \frac{(-1)^{\frac{\ell-3}{2}} \mathsf{P}}{\mathsf{R}}$$

Der zweite Faktor $h_1 = \frac{(-1)^{\frac{\ell-3}{2}} \mathsf{P}}{\mathsf{R}}$ ist die Klassenzahl des reellen Unterkörpers der zweigliedrigen Perioden vom Grade $\frac{\ell-1}{2}$.

Anmerkung für späteres Nachschlagen

Die entwickelten Formeln sind, soweit möglich numerisch geprüft und richtig befunden, insbesondere alle Vorzeichen. Speziell ergab sich für den Kreiskörper der 5–ten Einheitswurzeln $h = 1$.

1.10 Beweis des Eisensteinschen Reziprozitätsgesetzes. (31.7.1923)

Originally Eisenstein's reciprocity law was a necessary ingredient in the proofs of the higher reciprocity laws for a prime exponent ℓ (Kummer, Furtwängler, Takagi). Hasse gives an exposition of the prime ideal decomposition of Gauss sums and of Eisenstein's reciprocity law following Hilbert's presentation in his Zahlbericht [Hil98]*. ("Gauss sums" are called "Lagrangesche Wurzelzahlen".) Later in 1927 Hasse published a generalization of Eisenstein's reciprocity law for arbitrary exponent m* [Has27a]*. (But note that in the same year Artin succeeded to prove his general reciprocity law without resorting to Eisenstein's reciprocity law.) See also* [LR06]*, 6.3 and 9.4.*

I, 77

(Nach Hilbert, Zahlbericht.) 31. VII. 23.

a.) Die Lagrangesche Wurzelzahl.

Wir betrachten nebeneinander zwei Kreiskörper:

1.) Den Kreiskörper k_ζ der primitiven ℓ–ten Einheitswurzel ζ. s sei die erzeugende Substitution dieses Körpers und $s = (\zeta : \zeta^r)$.

2.) Den Kreiskörper k_{Z} der primitiven p–ten Einheitswurzel Z, wobei p eine Primzahl $\equiv 1 \mod. \ell$ ist. $\mathsf{S} = (\mathsf{Z} : \mathsf{Z}^{\mathsf{R}})$ sei seine erzeugende Substitution.

Der Körper $K = (k_\zeta, k_{\mathsf{Z}})$ ist dann ein Abelscher Körper vom Grade $(\ell-1)(p-1)$, dessen Gruppe offensichtlich das direkte Produkt $s^\nu \mathsf{S}^{\mathsf{N}}$ der beiden zyklischen Gruppen ist. k_ζ gehört zur Untergruppe S^{N} die ζ festläßt.

Man nennt die Zahl

$$\Lambda = \mathsf{Z} + \zeta \mathsf{Z}^{\mathsf{R}} + \zeta^2 \mathsf{Z}^{\mathsf{R}^2} + \cdots + \zeta^{p-2} \mathsf{Z}^{\mathsf{R}^{p-2}}$$

aus K eine *Lagrangesche Wurzelzahl.*

Bildet man

$$\mathsf{S}\Lambda = \mathsf{Z}^{\mathsf{R}} + \zeta \mathsf{Z}^{\mathsf{R}^2} + \zeta^2 \mathsf{Z}^{\mathsf{R}^3} + \cdots + \zeta^{p-3} \mathsf{Z}^{\mathsf{R}^{p-2}} + \zeta^{p-2} \mathsf{Z}$$

so folgt sofort, wegen $p - 2 \equiv -1 \mod \ell$:

$$\mathsf{S}\,\Lambda = \zeta^{-1}\Lambda$$

Also gilt[1] I, 81

$$\mathsf{S}\Lambda^\ell = \Lambda^\ell,$$

d. h.

$$\Lambda^\ell = \pi$$

ist Zahl aus k_ζ. Die Zahl Λ definiert somit einen relativ–zyklischen Körper k_Λ vom Primzahlgrad ℓ über k_ζ. Dieser Körper k_Λ gehört als Unterkörper von K über k_ζ ersichtlich zur Untergruppe

$$\mathfrak{G} = 1,\, \mathsf{S}^\ell,\, \mathsf{S}^{2\ell},\, \dots,\, \mathsf{S}^{(m-1)\ell},$$

wenn

$$p - 1 = m\ell$$

gesetzt wird. Denn einzig und allein diese Substitutionen der Galoisschen Gruppe S^N von K nach k_ζ lassen nach obigem Λ ungeändert.

Die Zahl Λ gibt ferner auf folgende Weise Anlaß zu einem weiteren Körper k_λ:

Schreibt man Λ in der Form: I, 82

$$\begin{array}{rlcccc} \Lambda & = & (\mathsf{Z} & + \quad \mathsf{Z}^{\mathsf{R}^\ell} & + \cdots + & \mathsf{Z}^{\mathsf{R}^{(m-1)\ell}}) \\ & + & \zeta(\mathsf{Z}^\mathsf{R} & + \quad \mathsf{Z}^{\mathsf{R}^{\ell+1}} & + \cdots + & \mathsf{Z}^{\mathsf{R}^{(m-1)\ell+1}}) \\ & & \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ & + & \zeta^{\ell-1}(\mathsf{Z}^{\mathsf{R}^{\ell-1}} & + \quad \mathsf{Z}^{\mathsf{R}^{\ell+(\ell-1)}} & + \cdots + & \mathsf{Z}^{\mathsf{R}^{(m-1)\ell+(\ell-1)}}) \\ & & & & & \\ & = & \lambda_0 & + \quad \zeta\lambda_1 & + \cdots + & \zeta^{\ell-1}\lambda_{\ell-1}\,, \end{array}$$

so genügen die ℓ Zahlen λ_i aus k_Z (die ℓ $m$gliedrigen Perioden von k_Z) der Bedingung:

$$\mathsf{S}^i\lambda_0 = \lambda_i\,; \quad (i = 0, 1, \dots \ell - 1) \tag{1}$$

während

$$\mathsf{S}^\ell\lambda_i = \lambda_i \tag{2}$$

ist. λ_0 definiert also nach (2) einen zur Untergruppe $\mathfrak{G}$ gehörigen Unterkörper k_λ über R, dessen Galoisgruppe die durch die Faktorgruppe $1, \mathsf{S}, \dots \mathsf{S}^{\ell-1}$ bewirkte

[1] Hasse has deleted pages 78-80 of his notebook I.

Permutationsgruppe der λ_i, also nach (1) zyklisch vom Grade ℓ ist. k_λ ist somit zyklischer Körper ℓ–ten Grades über R, und die λ_i sind konjugiert.

(Ist übrigens k ein zyklischer Körper, dessen Grad die ungerade Primzahl ℓ und dessen Diskriminante nur durch eine einzige Primzahl $p \neq \ell$ teilbar ist, so ist diese Diskriminante nach der Theorie des Galoisschen Körpers $-p^{\ell-1}$. (Reeller Körper: positive Diskr.) Nach S. 54], (14) ist sie ferner das Produkt der sämtlichen Führer der Charaktere der Klassengruppe aus R, nach der k Klassenkörper ist, Daraus folgt, daß diese Klassengruppe notwendig $(\ell - 1)$ Charaktere vom Führer p neben dem Hauptcharakter haben muß und folglich die Gruppe der Restklassen mod. p ist. k ist somit Unterkörper des umfassendsten Klassenkörpers nach dem Führer p, des Körpers k_{Z}, und da dieser nur für $p \equiv 1$ mod ℓ und nur einen Unterkörper ℓ–ten Grades besitzen kann (Gruppe!) ist k mit dem oben betrachteten Periodenkörper k_λ identisch:

I, 83

Satz 1: *Jeder zyklische Körper k vom Prinzahlgrad ℓ, dessen Diskriminante nur durch eine einzige Primzahl $p \neq \ell$ (beide ungerade) teilbar ist, ist mit dem Körper der ℓ m–gliedrigen Kreisteilungsperioden der Primzahl p identisch, (also $p - 1 = m\ell$).*

Hilbert geht von einem solchen Körper k als Ausgangspunkt aus. Jedoch scheint mir logischer, k_ζ an die Spitze zu stellen, da doch in k_ζ etwas bewiesen werden soll).

Wie man sofort sieht, bilden die konjugierten λ_i eine Basis, also eine *Normalbasis* für k_λ. Denn zunächst hat jede ganze Zahl aus k_{Z} die Basisdarstellung:

$$\mathsf{A} = a_0\mathsf{Z} + a_1\mathsf{Z}^{\mathsf{R}} + \cdots + a_{\mu-2}\mathsf{Z}^{\mathsf{R}^{p-2}}.$$

I, 84

Soll A zu k_λ gehören, so muß es die Substitutionen $1, \mathsf{S}^\ell, \mathsf{S}^{2\ell}, \ldots \mathsf{S}^{(m-1)\ell}$ von $\mathfrak{G}$ gestatten, woraus wegen der Eindeutigkeit der Basisdarstellung sofort folgt, daß in A die in einer Periode λ_i vorkommenden $\mathsf{Z}^{\mathsf{R}^\nu}$ gleiche Koeffizienten haben müssen. Also ist jede ganze Zahl A aus k_λ durch $\lambda_0, \ldots \lambda_{\ell-1}$ ganzzahlig darstellbar, w. z. b. w.

Aus dieser Tatsache folgt nun sofort Wichtiges über die *Lagrangesche Wurzelzahl Λ von k_λ*, (wie die Bezeichnung genau ist). (Λ ist nämlich eine spezielle, besonders einfache „Wurzelzahl" für den an sich nicht reinen zyklischen Körper, d. h. eine solche Zahl, durch die k_λ über k_ζ als Grundkörper betrachtet, erzeugt wird auf Grund der nunmehr *reinen* Gleichung $x^\ell = \pi$. Tatsächlich ist $(k_\lambda, k_\zeta) = k_\Lambda$, da Λ aus den λ_i aus k_λ und ζ aus k_ζ gebildet ist, sodaß jedenfalls k_Λ Unterkörper von (k_λ, k_ζ) ist, andererseits aber k_Λ den Grad $(\ell-1)\ell$ und

(k_λ, k_ζ) höchstens den Grad $(\ell-1)\ell$ hat.). Bildet man nämlich die Determinante

$$\Delta = \begin{vmatrix} \lambda_0 & \lambda_1 & \cdots & \lambda_{\ell-1} \\ \lambda_{\ell-1} & \lambda_0 & \cdots & \lambda_{\ell-2} \\ \\ \lambda_1 & \lambda_2 & \cdots & \lambda_0 \end{vmatrix} ,$$

so steht in der ersten Zeile die Basis von k_λ in der i–ten Zeile die durch S^{-i} erzeugte konjugierte Basis, sodaß Δ^2 die Diskriminante von k_λ also I, 85

$$\Delta^2 = -p^{\ell-1}$$

ist. Andererseits ist nach dem Gruppensatz von S. 69]

$$\Delta = \prod_{\mu=0}^{\ell-1} \sum_{\nu=0}^{\ell-1} \zeta^{\nu\mu} \lambda_\nu$$

da die λ_i in ihrer natürlichen Reihenfolge den Gruppenelementen der zyklischen Gruppe zugeordnet in Δ als Gruppendeterminante auftreten, und der μ–te, λ_ν zugeordnete Gruppencharakter dann $\zeta^{\nu\mu}$ ist. Es ist also:

$$\Delta = (\lambda_0 + \lambda_1 + \cdots + \lambda_{\ell-1}) \cdot \Lambda \cdot s\Lambda \cdots s^{\ell-2}\Lambda$$

oder, da der erste Faktor -1 ist:

$$\Lambda \cdot s\Lambda \cdots s^{\ell-2}\Lambda = \pm p^{\frac{\ell-1}{2}}$$

Geht man zur ℓ–ten Potenz über, so folgt:

$$\pi \cdot s\pi \cdots s^{\ell-2}\pi = N_{k_\zeta}(\pi) = p^{\frac{\ell(\ell-1)}{2}} ,$$

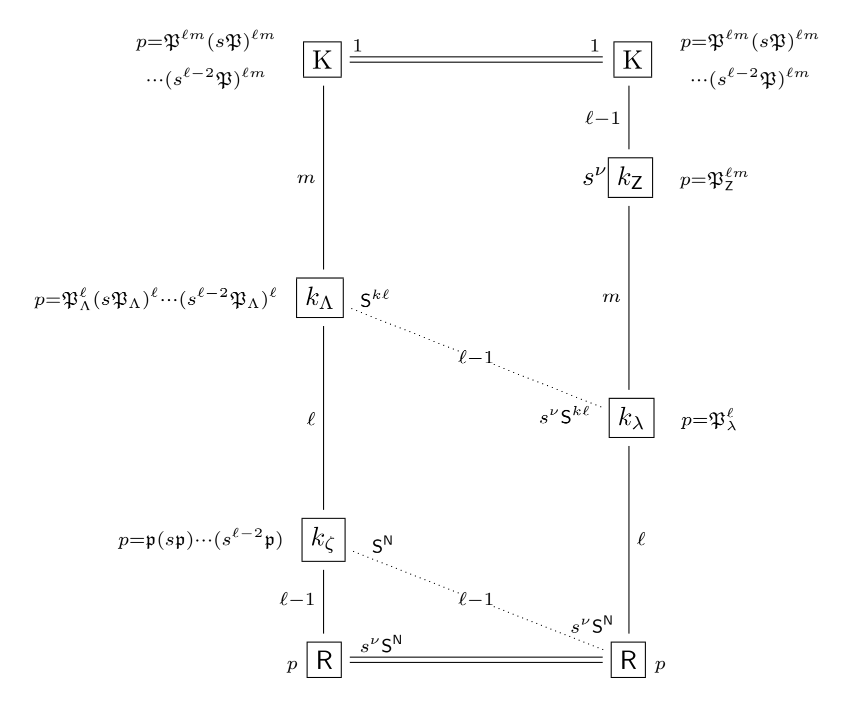
(da $N_{k_\zeta}(\pi)$ als Norm aus dem total imaginären Kreiskörper positiv sein muß). Wir haben also:

Satz 2. *Die ℓ–te Potenz $\Lambda^\ell = \pi$ der Lagrangeschen Wurzelzahl Λ von k_λ ist eine nur durch Primteiler von p teilbare Zahl aus k_ζ.*

Ich wende mich nunmehr zur Angabe der genauen Zerlegung von π in Primideale. I, 86

b.) Zerlegung der ℓ–ten Potenz der Lagrangeschen Wurzelzahl in Primideale.

Ich gebe zunächst eine bildliche Darstellung der in Frage kommenden Körper und der in ihnen herrschenden Zerlegung der Primzahl p:



Links und rechts ist je eine vom gemeinsamen Grundkörper R zum gemeinsamen Oberkörper K aufsteigende Körperreihe angegeben. Die Längen der Verbindungsstrecken entsprechen den (angeschriebenen) Relativgraden. Jeder Körper ist zyklisch zum darunterstehenden. Auf der Innenseite sind die Gruppen angegeben, zu denen die Körper als Unterkörper von K über R gehören. Da K Abelsch ist, sind es auch alle seine Unterkörper. Nun gilt bekanntlich in K die Zerlegung

I, 87

$$p = \mathfrak{P}^{\ell m}(s\mathfrak{P})^{\ell m}\cdots(s^{\ell-2}\mathfrak{P})^{\ell m}; \quad \text{(Grade hier wie überall 1)}$$

Denn einerseits muß p sicher in mindestens $\ell-1$ verschiedenen Primteilerpotenzen zerfallen, da dies wegen $p \equiv 1 \mod \ell$ schon im Unterkörper k_ζ gilt, andererseits muß die Ordnung der Primteiler mindestens $\ell m = p-1$ sein, da dies schon im Unterkörper k_{Z} gilt. Also folgt wegen $(\ell-1)\ell m = (p-1)(\ell-1) =$ Grad von K, d. h. beide Zahlen tatsächlich die wahren und der Grad von $\mathfrak{P}$ gleich 1

ist. Da der Grad der Zerlegungsgruppe nunmehr zu ℓm, also ihr Index zu $\ell - 1$ erkannt ist, folgt, daß der Körper k_ζ vom Grade $\ell - 1$, der nach der allgemeinen Theorie Unterkörper des Zerlegungskörpers ist, dieser selbst sein muß. Somit sind $\mathfrak{P}$, $s\mathfrak{P}, \dots\ s^{\ell-2}\mathfrak{P}$ die konjugierten Primteiler, da S^{N} die Zerlegungsgruppe. Die übrigen angegebenen Zerlegungen ergeben sich nun leicht aus der bekannten Zerlegung im Abelschen Oberkörper und den Gruppen zu denen jene Körper gehören.

Speziell ist das Primideal $\mathfrak{P}_{\mathsf{Z}}$ bekanntlich

$$\mathfrak{P}_{\mathsf{Z}} = (1 - \mathsf{Z}) = (\Pi)$$

Also gilt in K folgende Zerlegung

$$-\Pi = 1 - \mathsf{Z} = \mathfrak{P}\,(s\mathfrak{P}) \dots (s^{\ell-2}\mathfrak{P}),$$

sodaß Π durch jeden der Primteiler $s^i\mathfrak{P}$ von p in K genau einmal teilbar ist. I, 88
Diese Bemerkung dient zur Herleitung der Potenzen der $s^i\mathfrak{P}$, die in Λ aufgehen.

Ist nämlich

$$\mathfrak{p} = (p, \zeta - \mathsf{R}^{-m})$$

ein bestimmter der Primteiler von p in k_ζ, der ja wegen $p \equiv 1 \mod. \ell$, also

$$f(x) = x^{\ell-1} + \dots + x + 1 = \frac{x^\ell - 1}{x - 1} \equiv (x - \mathsf{R}^{-m})(x - \mathsf{R}^{-2m}) \dots \\ \dots (x - \mathsf{R}^{-(\ell-1)m}) \mod p$$

$\big(\mathsf{R}^{-m}, \dots, \mathsf{R}^{-(\ell-1)m}$ sind mod p die sämtlichen primitiven ℓ–ten Einheitswurzeln$\big)$ in dieser Form angesetzt werden darf, so gilt

$$\zeta \equiv \mathsf{R}^{-m} \mod \mathfrak{p},$$

ebenso

$$s^i\zeta = \zeta^{r^i} \equiv \mathsf{R}^{-m} \mod s^i\mathfrak{p},$$

d. h.

$$\zeta \equiv \mathsf{R}^{-mr^{-i}} \mod s^i\mathfrak{p}.$$

Daher ist, wegen $\mathfrak{P}^{m\ell} = \mathfrak{p}$:

$$\Lambda = \sum_{\nu=0}^{p-2} \zeta^\nu \mathsf{Z}^{\mathsf{R}^\nu} \equiv \sum_{\nu=0}^{p-2} \mathsf{R}^{-m\nu} \mathsf{Z}^{\mathsf{R}^\nu} \equiv \sum_{\kappa=1}^{p-1} \kappa^{-m} \mathsf{Z}^\kappa \mod \mathfrak{P}^{m\ell}$$

Setzt man dann $\mathsf{Z} = 1 + \Pi$, so folgt

$$\Lambda \equiv \sum_{\kappa=1}^{p-1} \kappa^{-m} \sum_{\mu=0}^{\kappa} \binom{\kappa}{\mu} \Pi^\mu \equiv \sum_{\mu=0}^{p-1} \Pi^\mu \sum_{\kappa=1}^{p-1} \binom{\kappa}{\mu} \kappa^{-m} \quad \text{mod } \mathfrak{P}^{m\ell}$$

Nun ist ersichtlich wegen $0 \leqq \mu \leqq p-1$ der Binomialkoeffizient $\binom{\kappa}{\mu}$ ein Polynom

I, 89 μ–ten Grades in κ mit mod. p ganzzahligen Koeffizienten. Ferner gilt:

$$\sum_{\kappa=1}^{p-1} \kappa^\nu \equiv \left\{ \begin{array}{lllllll} 0 & \text{mod} & p\,, & \text{wenn} & \nu \not\equiv 0 & \text{mod} & (p-1) \\ -1 & " & " & " & \nu \equiv 0 & " & " \end{array} \right\}$$

Für $\mu = 0$ ist stets $\binom{\kappa}{0} = 1$ und wegen $m \not\equiv 0 \mod (p-1)$ sicher der Koeffizient von Π^0 durch p teilbar. Für $\mu \geqq 1$ treten in $\binom{\kappa}{\mu}$ nur die Potenzen $\kappa, \kappa^2, \ldots, \kappa^\mu$ auf, also im Koeffizienten von Π^μ nur die Summen über die Potenzen $\kappa^{1-m}, \kappa^{2-m}, \ldots, \kappa^{\mu-m}$. Ist daher $1 \leqq \mu < m$, so ist keine der entsprechenden $\sum_{\kappa=1}^{p-1} \equiv -1 \mod p$, d. h. alle Glieder bis Π^{m-1} haben Koeffizienten $\equiv 0 \mod p$, d. h. fallen mod $\mathfrak{P}^{m\ell}$ heraus. Im Gliede mit Π^m dagegen, lauten die entsprechenden Potenzen:

$$\kappa^{1-m}, \kappa^{2-m}, \ldots, \kappa^{m-m}$$

sodaß das letzte Glied allein einen Beitrag liefern wird, der sich sofort zu $-\frac{1}{m!}$ herausstellt. Es ist also:

$$\Lambda \equiv -\frac{\Pi^m}{m!} \quad \text{mod } \mathfrak{P}^{m+1}$$

d. h. Λ genau durch $\mathfrak{P}^m$ und somit $\pi = \Lambda^\ell$ genau durch $\mathfrak{P}^{m\ell} = \mathfrak{p}$ teilbar.

Ebenso untersuchen wir die Teilbarkeit von $\Lambda^\ell = \pi$ durch die konjugierten $s^i\mathfrak{p}\,;\ (i = 1, 2, \ldots \ell - 2)$. Es wird nach obigem

$$\begin{aligned} \Lambda \quad &\equiv \quad \sum_{\nu=0}^{p-2} \mathsf{R}^{-mr^{-i}\nu} \mathsf{Z}^{\mathsf{R}^\nu} \quad \text{mod } (s^i\mathfrak{P})^{\ell m}, \quad \text{und ebenso wie oben:} \\ \Lambda \quad &\equiv \quad \sum_{\mu=0}^{p-1} \Pi^\mu \sum_{\kappa=1}^{p-1} \binom{\kappa}{\mu} \kappa^{-mr^{-i}} \quad \text{mod } (s^i\mathfrak{P})^{\ell m} \end{aligned}$$

I, 90 Der Koeffizient von Π^0 ist wie oben $\equiv 0$ mod. p. Für den Koeffizienten von Π^μ

für $\mu \geqq 1$ kommt es auf die Summen über

$$\kappa^{1-mr^{-i}},\ \kappa^{2-mr^{-i}},\ldots,\ \kappa^{\mu-mr^{-i}}$$

an. Wann kann nun

$$\nu - mr^{-i} \equiv 0 \mod (p-1)$$

sein? Dazu muß wegen $p-1 = m\ell$ zunächst $\nu = m\nu_0$ ein Vielfaches von m sein. Ferner

$$\nu_0 \equiv r^{-i} \text{ mod. } \ell$$

Für alle ν_0 von 1 bis zu $r_{-i}-1$, wenn r_{-i} den kleinsten positiven Rest von $r^{-i} \mod \ell$ bezeichnet, ist dies nicht der Fall, somit sind alle Koeffizienten bis $\Pi^{(r_{-i}-1)m}$ kongruent Null mod. p. Für $\mu = r_{-i}m$ ist nur die letzte κ Potenz κ^0, somit der Koeffizient von $\Pi^{r_{-i}m}$ gleich $-\frac{1}{(r_{-i}m)!}$ mod. p. Es wird also

$$\Lambda \equiv -\frac{\Pi^{r_{-i}m}}{(r_{-i}m)!} \mod (s^i\mathfrak{P})^{r_{-i}m+1}$$

d. h. Λ genau durch $(s^i\mathfrak{P})^{r_{-i}m}$, also $\Lambda^\ell = \pi$ genau durch $(s^i\mathfrak{P})^{r_{-i}\ell m} = (s^i\mathfrak{p})^{r_{-i}}$ teilbar. Daher gilt:

Satz 3. *Die ℓ–te Potenz π der Lagrangeschen Wurzelzahl Λ hat in k_ζ die Primidealzerlegung:*

$$\pi = \mathfrak{p}^{r_0+r_{-1}s+r_{-2}s^2+\cdots+r_{-(\ell-2)}s^{\ell-2}}$$

wenn r_i den kleinsten positiven Rest von $r^i \mod \ell$ bezeichnet. Λ selbst zerfällt dann also in k_Λ so:

$$\Lambda = \mathfrak{P}_\Lambda^{r_0+r_{-1}s+\cdots+r_{-(\ell-2)}s^{\ell-2}}$$

Der bewiesene Satz steht mit $N_{k_\zeta}(\pi) = p^{\frac{\ell(\ell-1)}{2}}$ in Einklang, da sich ergibt: I, 91

$$N_{k_\zeta}(\pi) = p^{r_0+r_{-1}+\cdots+r_{-(\ell-2)}} = p^{1+2+\cdots+(\ell-1)} = p^{\frac{\ell(\ell-1)}{2}}.$$

Sieht man Satz 3 als reinen Satz in k_ζ an, so besagt er, daß zu dem Primideal $\mathfrak{p} = (p, \zeta - \mathsf{R}^{-m})$ aus k_ζ eine ganz bestimmte Funktion von s gehört, sodaß $\mathfrak{p}^{f(s)} \sim 1$ ist. I, 92

Dieselbe Äquivalenz besteht natürlich auch für die konjugierten $s^i\mathfrak{p}$, denn es folgt eben durch Erheben in die s–te Potenz $\mathfrak{p}^{sf(s)} \sim 1$, d. h. $(s\mathfrak{p})^{f(s)} \sim 1$.

Da $\mathfrak{p}$ ein beliebiges Primideal 1. Grades sein kann und in jeder Klasse solche vorkommen, gilt somit ganz allgemein:

Satz 4. *Bezeichnet $f(s)$ die symbolische Funktion*

$$f(s) = r_0 + r_{-1}s + \cdots + r_{-(\ell-2)}s^{\ell-2}$$

mit den Bezeichnungen von Satz 3, so gilt für jede Idealklasse C von k_ζ die Äquivalenz

$$C^{f(s)} = 1.$$

Diese Äquivalenz kann noch weiter reduziert werden; es ist nämlich

$$\Lambda^{s-r} = \frac{s\Lambda}{\Lambda^r};$$

$$\mathsf{S}(\Lambda^{s-r}) = \frac{\mathsf{S}(s\Lambda)}{\mathsf{S}\Lambda^r} = \frac{s(\mathsf{S}\Lambda)}{\mathsf{S}\Lambda^r} = \frac{s(\zeta^{-1}\Lambda)}{\zeta^{-r}\Lambda^r} = \frac{s\Lambda}{\Lambda^r}$$

I, 93 also Λ^{s-r} Zahl aus k_ζ. Daher ist $\pi^{s-r} = \Lambda^{\ell(s-r)}$ ℓ–te Potenz einer Zahl aus k_ζ und somit

$$\begin{aligned} \mathfrak{p}^{(s-r)f(s)} &= \mathfrak{p}^{(r_1-rr_0)+(r_0-rr_{-1})s+\cdots+(r_{-(\ell-3)}-rr_{-(\ell-2)})s^{\ell-2}} \\ &= \alpha^\ell \end{aligned}$$

(dabei ist $r_1 = r_{-(\ell-2)}$ zu berücksichtigen). *Natürlich* sind die Exponenten der einzelnen Primteilerpotenzen durch ℓ teilbar, wesentlich ist nur die neue Erkenntnis, daß ein Hauptideal als ℓ–te Wurzel herauskommt. Dreht man alle Vorzeichen um, so ist $\frac{rr_{-i}-r_{-(i-1)}}{\ell} = q_{-i}$ überdies stets positiv und man hat, genau wie oben:

Satz 5. *Für jede Idealklasse C von k_ζ besteht die Beziehung*

$$C^{Q(s)} = 1,$$

wenn $Q(s) = q_0 + sq_{-1} + s^2q_{-2} + \cdots + s^{\ell-2}q_{\ell-2}$ gesetzt wird und die q_{-i} wie angegeben als positive ganze Zahlen definiert werden.

c.) Der Potenzrestcharakter der Lagrangeschen Wurzelzahl.

Sei unter Beibehaltung der bisherigen Bezeichnungen q eine beliebige von ℓ, p verschiedene Primzahl, $\mathfrak{q}$ ein Primteiler von q in k_ζ vom Grade $\mathfrak{f}$. Dann

I, 94 bilden wir durch sukzessives Potenzieren mit q die Kongruenz:

$$\Lambda^{q^\mathfrak{f}} \equiv \mathsf{Z}^{q^\mathfrak{f}} + \zeta^{q^\mathfrak{f}}\mathsf{Z}^{\mathsf{R}q^\mathfrak{f}} + \cdots + \zeta^{(p-2)q^\mathfrak{f}}\mathsf{Z}^{\mathsf{R}^{p-2}q^\mathfrak{f}} \mod. q$$

Wegen $q^{\mathfrak{f}} \equiv 1 \mod \ell$, und wenn $q^{\mathfrak{f}} \equiv \mathsf{R}^h \mod p$ gesetzt wird, folgt:

$$\Lambda^{q^{\mathfrak{f}}} \equiv \mathsf{Z}^{\mathsf{R}^h} + \zeta \mathsf{Z}^{\mathsf{R}^{h+1}} + \cdots + \zeta^{(p-2)} \mathsf{Z}^{\mathsf{R}^{h+(p-2)}} = \zeta^{-h} \Lambda \mod q.$$

Da Λ prim zu q ist, ist daher

$$\Lambda^{q^{\mathfrak{f}}-1} = \Lambda^{N(\mathfrak{q})-1} \equiv \zeta^{-h} \mod q$$

also

$$\pi^{\frac{N(\mathfrak{q})-1}{\ell}} \equiv \zeta^{-h} \mod q$$

wenn N die Norm in k_ζ bezeichnet. Das besagt:

$$\left(\frac{\pi}{\mathfrak{q}}\right) = \zeta^{-h}.$$

Andererseits folgt:

$$q^{\mathfrak{f}\frac{p-1}{\ell}} \equiv \mathsf{R}^{h\frac{p-1}{\ell}} = \mathsf{R}^{hm} \equiv \zeta^{-h} \mod \mathfrak{p}$$

weil $\zeta \equiv \mathsf{R}^{-m} \mod \mathfrak{p}$ ist. Daher ist

$$\left(\frac{q^{\mathfrak{f}}}{\mathfrak{p}}\right) = \left(\frac{N(\mathfrak{q})}{\mathfrak{p}}\right) = \zeta^{-h},$$

also:

Satz 6. *Für die ℓ–te Potenz $\pi = \Lambda^\ell$ der Lagrangeschen Wurzelzahl, das Primideal $\mathfrak{p} = (p, \zeta - \mathsf{R}^{-m})$, welches ihr zugeordnet ist, (durch welches π genau einmal teilbar ist), und ein beliebiges Primideal $\mathfrak{q}$ aus k_ζ das zu p und ℓ prim ist, gilt die Reziprozitätsbeziehung:*

$$\left(\frac{\pi}{\mathfrak{q}}\right) = \left(\frac{N\,\mathfrak{q}}{\mathfrak{p}}\right)$$

Anmerkung: Dieser Satz ist etwa so zu verstehen: Zu jeder Primzahl $p \equiv 1 \mod \ell$ gibt es einen (oder mehrere) Primteiler der speziellen Struktur $\mathfrak{p} = (p, \zeta - \mathsf{R}^{-m})$, wo R eine Primitivzahl nach p und $p - 1 = m\ell$ ist. Jedem solchen $\mathfrak{p}$ entspricht eine mit diesem R und ζ gebildete Lagrangesche Wurzelzahl Λ, deren ℓ–te Potenz $\Lambda^\ell = \pi$ jenes $\mathfrak{p}$ *als einzigen* der konjugierten Primteiler ein einziges mal enthält, während alle anderen in höheren Potenzen aufgehen. Auf diese speziellen $\mathfrak{p}$ und eindeutig zugeordneten Zahlen π bezieht sich unser Hilfssatz, der den wesentlichsten Teil des Eisensteinschen Reziprozitätsgesetzes enthält.

I, 95

d.) Beweis des Eisensteinschen Gesetzes.

Ist $\mathfrak{l} = (1-\zeta) = \lambda$, so heißt eine beliebige Zahl α aus k_ζ *semiprimär*, wenn sie prim zu $\mathfrak{l}$ und kongruent einer rationalen Zahl nach $\mathfrak{l}^2$ ist. Sie muß also eine Entwicklung:

$$\alpha = a_0 + a_2\lambda^2 + \cdots \ (\mathfrak{l})\,; \quad \big(a_0 \not\equiv 0 \ (\ell)\big)$$

haben.

Ist $\beta = b_0 + b_1\lambda + \cdots$ eine beliebige zu $\mathfrak{l}$ prime Zahl aus k_ζ , so ist

$$\begin{aligned} \zeta^c\beta &= b_0\zeta^c + b_1\lambda + \cdots \\ \\ &= b_0 - cb_0\lambda + b_1\lambda + \cdots \\ &= b_0 + (b_1 - cb_0)\lambda + \cdots \end{aligned}$$

I, 96 also wegen $b_0 \not\equiv 0 \mod. \ell$ für ein ganz bestimmtes c semiprimär. Die zu beweisende Behauptung lautet:

$$\left(\frac{a}{\alpha}\right) = \left(\frac{\alpha}{a}\right),$$

wenn a rational, prim zu ℓ, α semiprimär, prim zu a.

Beweis: Sei zunächst a eine rationale Primzahl $q \neq \ell$. Ist der Satz für jedes $q \neq \ell$ bewiesen, so folgt vermöge der Eigenschaften des Legendre–Symbols seine allgemeine Gültigkeit. Ferner nehmen wir vorerst an, α enthalte nur Primideale ersten Grades.

Sei wieder $\mathfrak{q}$ ein Primteiler von q, sein Grad $\mathfrak{f}$, ferner p eine in $N(\alpha)$ vorkommende rationale Primzahl, also n. Annahme $p \equiv 1 \mod. \ell$ und $\mathfrak{p}$ und π die oben eingeführten, p entsprechenden Größen. Nach Satz 6 ist dann

$$\left(\frac{\pi}{s^{-i}\mathfrak{q}}\right) = \left(\frac{q}{\mathfrak{p}}\right)^{\mathfrak{f}}$$

also, wenn s^i angewendet wird:

$$\left(\frac{s^i\pi}{\mathfrak{q}}\right) = \left(\frac{q}{s^i\mathfrak{p}}\right)^{\mathfrak{f}}$$

Diese Gleichung soll Verwendung finden, um $\left(\frac{\alpha}{q}\right)$ vermöge einer Zerlegung einer symbolischen Potenz von α in Faktoren der Form $s^i\pi$ auszudrücken.

Seien dazu $p, p', \dots$ die verschiedenen in $N(\alpha)$ vorkommenden Primzahlen, also $p = m\ell+1$, $p' = m'\ell+1$, ... ferner $\mathsf{R}, \mathsf{R}', \dots$ Primitivzahlen für sie, $\mathfrak{p}, \mathfrak{p}', \dots$ die in obiger Weise gebildeten Primideale und $\pi = \Lambda^\ell$, $\pi' = {\Lambda'}^\ell$, ... die zugehörigen ℓ–ten Potenzen der Lagrangeschen Wurzelzahlen. Es gilt dann einerseits: I, 97

$$\alpha = \mathfrak{p}^{F(s)} {\mathfrak{p}'}^{F'(s)} \dots$$

mit ganzzahligen Funktionen $(\ell - 2)$ ten Grades von s sind, andererseits nach Satz 3

$$\begin{array}{lcl} \pi & = & \mathfrak{p}^{r_0 + r_{-1}s + \dots + r_{-(\ell-2)}s^{\ell-2}}, \\ \pi' & = & {\mathfrak{p}'}^{r_0 + r_{-1}s + \dots + r_{-(\ell-2)}s^{\ell-2}}, \\ \dots & \dots & \dots\dots\dots\dots\dots\dots \end{array}$$

Daraus bilden wir die Zahl:

$$\varepsilon = \frac{\alpha^{r_0 + r_{-1}s + \dots + r_{-(\ell-2)}s^{\ell-2}}}{\pi^{F(s)} {\pi'}^{F'(s)} \dots}$$

die offenbar Einheit aus k_ζ ist. Wir können jedoch sogar zeigen, daß $\varepsilon = \pm 1$ sein muß. Es gilt nämlich zunächst:

Satz 7. *Die Lagrangesche Wurzelzahl Λ zu p hat den absoluten Betrag $\sqrt{p}$.*

Beweis:

Es ist I, 98

$$\begin{aligned} |\Lambda|^2 = \Lambda\overline{\Lambda} &= \sum_{\nu=0}^{p-2} \zeta^\nu \mathsf{Z}^{\mathsf{R}^\nu} \cdot \sum_{\mu=0}^{p-2} \zeta^{-\mu} \mathsf{Z}^{-\mathsf{R}^\mu} \\ &= \sum_{\kappa=0}^{p-2} \zeta^\kappa \sum_{\mu=0}^{p-2} \mathsf{Z}^{\mathsf{R}^{\kappa+\mu} - \mathsf{R}^\mu} \\ &= \sum_{\kappa=0}^{p-2} \zeta^\kappa \sum_{\mu=0}^{p-2} \mathsf{Z}^{\mathsf{R}^\mu(\mathsf{R}^\kappa - 1)} \end{aligned}$$

Die innere Summe ist als Summe *aller* Potenzen von $\mathsf{Z}^{\mathsf{R}^\mu - 1}$ entweder $p - 1$, wenn $\mathsf{R}^\kappa - 1 \equiv 0 \mod p$, d. h. für $\kappa = 0$, sonst -1, daher

$$|\Lambda|^2 = p - 1 - (\zeta + \zeta^2 + \dots + \zeta^{p-2}).$$

Nun ist letztere ζ–Summe, wenn man sie in Abschnitte von $\ell, \ell, \dots, \ell, \ell - 1$ Gliedern einteilt, gleich -1, also

$$|\Lambda|^2 = p\,, \quad \text{w. z. b. w.}$$

Wenden wir dies auf unser ε an, so wird

$$|\varepsilon|^2 = \varepsilon\overline{\varepsilon} = \varepsilon\varepsilon^{1+s^{\frac{\ell-1}{2}}} = \frac{\alpha^{(1+s^{\frac{\ell-2}{2}})(r_0+r_{-1}s+\cdots+r_{-(\ell-2)}s^{\ell-2})}}{\left(|\pi|^2\right)^{F(s)}\left(|\pi'|^2\right)^{F'(s)}\cdots}$$

Der Zähler rechts wird wegen:

$$\begin{aligned}&\left(1+s^{\frac{\ell-1}{2}}\right)\left(r_0+r_{-1}s+\cdots+r_{-(\ell-2)}s^{\ell-2}\right)\\ =&\left(r_0+r_{-\frac{\ell-1}{2}}\right)+\left(r_{-1}+r_{-1-\frac{\ell-1}{2}}\right)s+\cdots+\left(r_{-(\ell-2)}+r_{-(\ell-2)-\frac{\ell-1}{2}}\right)s^{\ell-2}\end{aligned}$$

und weil $r_{-i}+r_{-i-\frac{\ell-1}{2}}$ als Summe zweier mod. ℓ nur im Vorzeichen unterschiedener kleinster Reste den Wert ℓ hat:

I, 99

$$\alpha^{\ell(1+s+\cdots+s^{\ell-2})} = (N\alpha)^{\ell}.$$

Der Nenner wird nach Satz 7 gleich

$$p^{\ell F(s)}p'^{\ell F'(s)}\cdots\,,$$

oder da

$$\alpha = \mathfrak{p}^{F(s)}\mathfrak{p}'^{F'(s)}\cdots$$

ist, gleich $(N\alpha)^{\ell}$. Somit wird

$$|\varepsilon|^2 = 1$$

d. h. $$|\varepsilon| = 1$$

daher auch $$|s\varepsilon| = 1\,, \ \dots$$

also ε gleich $\pm\zeta^c$.

Nun ist zunächst für jede Lagrangesche Wurzelzahl:

$$\Lambda = \sum_{\nu=0}^{p-2}\zeta^{\nu}\mathsf{Z}^{\mathsf{R}^{\nu}} \equiv \sum_{\nu=0}^{p-2}\mathsf{Z}^{\mathsf{R}^{\nu}} \equiv -1 \mod \mathfrak{l}\,,$$

und daraus folgt wegen $\Lambda^\ell = \pi$:

$$(\pi+1) = (\Lambda^\ell + 1) = (\Lambda+1)(\zeta\Lambda+1)\cdots(\zeta^{\ell-1}\Lambda+1)\,,$$

also da

$$\begin{aligned} \zeta\Lambda+1 &\equiv \Lambda+1 \equiv 0 \mod \mathfrak{l} \\ \pi+1 &\equiv 0 \mod \mathfrak{l}^\ell \end{aligned}$$

also π semiprimär, ebenso $\pi', \dots$ da aber auch α semiprimär ist und jede (auch symbolische) Potenz sowohl als auch jedes Produkt semiprimärer Zahlen es wieder ist, auch ε semiprimär, mithin

$$\varepsilon = \pm 1\,,$$

also

$$\alpha^{r_0 + r_{-1}s + \cdots + r_{-(\ell-2)}s^{\ell-2}} = \pm \pi^{F(s)} \pi'^{F'(s)} \cdots$$

Die Anwendung der Formel auf S. 96] unten ergibt somit I, 100

$$\begin{aligned} \left(\frac{\alpha^{r_0 + r_{-1}s + \cdots + r_{-(\ell-2)}s^{\ell-2}}}{\mathfrak{q}}\right) &= \left(\frac{q}{\mathfrak{p}^{F(s)}\mathfrak{p}'^{F'(s)}\cdots}\right)^{\mathfrak{f}} \\ &= \left(\frac{q}{\alpha}\right)^{\mathfrak{f}}. \end{aligned}$$

(Es ist nämlich $\left(\frac{-1}{\mathfrak{q}}\right) = +1$).
Weiter ist aber

$$\begin{aligned} \left(\frac{s\alpha}{\mathfrak{q}}\right) &= s\left(\frac{\alpha}{s^{-1}\mathfrak{q}}\right) = \left(\frac{\alpha}{s^{-1}\mathfrak{q}}\right)^{r}, \\ \left(\frac{s^2\alpha}{\mathfrak{q}}\right) &= \left(\frac{\alpha}{s^{-2}\mathfrak{q}}\right)^{r^2}, \ \dots \end{aligned}$$

also

$$\left(\frac{\alpha^{r_{-i}s^i}}{\mathfrak{q}}\right) = \left(\frac{\alpha^{r_{-i}}}{s^{-i}\mathfrak{q}}\right)^{r^i} = \left(\frac{\alpha}{s^{-i}\mathfrak{q}}\right)^{r_{-i}r^i} = \left(\frac{\alpha}{s^{-i}\mathfrak{q}}\right)$$

somit

$$\left(\frac{\alpha}{N\mathfrak{q}}\right) = \left(\frac{q}{\alpha}\right)^{\mathfrak{f}}, \quad \text{d.h.} \quad \left(\frac{\alpha}{q}\right) = \left(\frac{q}{\alpha}\right)$$

weil ja $\mathfrak{f}$ als Teiler von $\ell-1$ prim zu ℓ ist. Damit ist der Satz unter der beschränkenden Voraussetzung für α bewiesen.

Um schließlich diese letzte Annahme zu befriedigen, sei α eine beliebige, semiprimäre zu $\mathfrak{q}$ prime Zahl aus k_ζ. Da nun für ein beliebiges Primideal $\mathfrak{p}$ vom Grade $\mathfrak{f} = \frac{\ell-1}{e}$ offenbar $s^e\mathfrak{p} = \mathfrak{p}$ ist, wird $\mathfrak{p}^{1-s^e} = 1$ für jedes Primideal dieses Typus. Also wird[2]

I, 104

$$\beta = \alpha^{\prod_e (1-s^e)},$$

wo e alle echten Teiler von $\ell-1$ durchläuft, so beschaffen sein, daß kein Primideal von höherem als dem ersten Grade mehr darin aufgeht; β ist ferner prim zu q und semiprimär, also

$$\left(\frac{\beta}{q}\right) = \left(\frac{q}{\beta}\right).$$

Da nun ferner

$$\left(\frac{s\alpha}{q}\right) = \left(\frac{\alpha}{q}\right)^r \quad \text{und} \quad \left(\frac{q}{s\alpha}\right) = \left(\frac{q}{\alpha}\right)^r,$$

somit

$$\left(\frac{\alpha^{F(s)}}{q}\right) = \left(\frac{\alpha}{q}\right)^{F(r)} \quad \text{und} \quad \left(\frac{q}{s\alpha}\right) = \left(\frac{q}{\alpha}\right)^{F(r)}$$

gilt, ist

$$\left(\frac{\beta}{q}\right) = \left(\frac{\alpha}{q}\right)^{\prod_e (1-r^e)},$$

$$\left(\frac{\beta}{q}\right) = \left(\frac{q}{\alpha}\right)^{\prod_e (1-r^e)}.$$

Da aber kein Faktor im Exponent durch ℓ teilbar sein kann, weil $e \neq \ell - 1$ vorausgesetzt wurde, folgt:

$$\left(\frac{\alpha}{q}\right) = \left(\frac{q}{\alpha}\right), \qquad \text{w. z. b. w.}$$

Satz 8. *Eisensteinsches Reziprozitätsgesetz. Ist a eine rationale, zu ℓ prime und α eine semiprimäre, zu a prime Zahl aus k_ζ, so ist*

$$\left(\frac{\alpha}{a}\right) = \left(\frac{a}{\alpha}\right)$$

[2]Die Seiten 101-103 sind im Tagebuch nicht vorhanden.

1.11 Einige Sätze über Einheiten und Klassenzahl des Kreiskörpers der ℓ–ten Einheitswurzeln. (9.8.1923)

Hasse follows Hilbert's Zahlbericht investigating the analytic class number formula for cyclotomic fields, in particular Kummer's condition for divisibility of the first factor by ℓ, connecting this with Bernoulli numbers, and the fundamental fact that ℓ must divide the first factor if it divides the second.

I, 105

(Nach Hilbert, Zahlbericht) 9. VIII. 23.

a.) Der erste Klassenzahlfaktor.

Der erste Faktor der Klassenzahl ist nach Satz 3, S. 76]

$$h_1 = (-1)^{\frac{\ell-1}{2}} \frac{\prod_{k=1,3,\ldots\,\ell-2} \sum_{\nu=1}^{\ell-1} \nu \varrho^{k\,\mathrm{ind}\,\nu}}{(2\ell)^{\frac{\ell-3}{2}}} \;,$$

wenn ϱ eine primitive $(\ell-1)$ te Einheitswurzel bezeichnet und die Indizes mod. ℓ in Bezug auf eine primitive Wurzel r mod. ℓ verstanden sind. Es soll die Teilbarkeit von h_1 durch ℓ untersucht werden.

Der Zähler ist von der Form

$$f(\varrho)\, f(\varrho^3) \ldots\, f(\varrho^{\ell-2}),$$

wobei

$$f(x) = \sum_{\nu=1}^{\ell-1} \nu x^{\mathrm{ind}\,\nu} = \sum_{\nu=0}^{\ell-2} r_\nu x^\nu$$

ist, und r_ν den kleinsten positiven Rest von r^ν mod. ℓ bezeichnet. Ich bilde nun

$$(r\varrho - 1) f(\varrho) = \sum_{\nu=0}^{\ell-2} r e_\nu \varrho^{\nu+1} - \sum_{\nu=0}^{\ell-2} r_\nu \varrho^\nu,$$

oder wegen $\varrho^{\ell-1} = 1,\ r_0 = r_{\ell-1} = 1$:

$$\begin{aligned}\big(r\varrho - 1, f(\varrho)\big) &= \sum_{\nu=0}^{\ell-2} r r_\nu \varrho^{\nu+1} - \sum_{\nu=0}^{\ell-2} r_{\nu+1}\varrho^{\nu+1} \\ &= \varrho \sum_{\nu=0}^{\ell-2} (r r_\nu - r_{\nu+1})\varrho^\nu\end{aligned}$$

I, 106

Nun ist $r r_\nu - r_{\nu+1} \equiv r r^\nu - r^{\nu+1} \equiv 0 \bmod. \ell$. Wird also

$$q_\nu = \frac{r r_\nu - r_{\nu+1}}{\ell}$$

gesetzt, so ist

$$(r\varrho - 1) f(\varrho) = \varrho\ell \sum_{\nu=0}^{\ell-2} q_\nu \varrho^\nu = \varrho\ell g(\varrho),$$

wo

$$g(x) = \sum_{\nu=0}^{\ell-2} q_\nu x^\nu$$

gesetzt ist. Ebenso ist natürlich

$$(r\varrho^i - 1) f(\varrho^i) = \varrho^i \ell g(\varrho^i)$$

also

$$\prod_{i=1,3,\dots\,\ell-2} (r\varrho^i - 1) f(\varrho^i) = \ell^{\frac{\ell-1}{2}} \varrho^{1+3+\dots+(\ell-2)} \prod_{i=1,3,\dots\,\ell-2} g(\varrho^i)$$

Nun ist

$$\varrho^{1+3+\dots+\ell-2} = \varrho^{\left(\frac{\ell-1}{2}\right)^2} = (-1)^{\frac{\ell-1}{2}}$$

ferner

$$(r\varrho - 1)(r\varrho^3 - 1)\dots(r\varrho^{\ell-2} - 1) = (-1)^{\frac{\ell-1}{2}} (r^{\frac{\ell-1}{2}} + 1),$$

denn es ist

$$y^{\ell-1} - 1 = (y^{\frac{\ell-1}{2}} - 1)(y^{\frac{\ell-1}{2}} + 1)$$

und die Größen $1, \varrho^2, \varrho^4, \dots\ \varrho^{\ell-3}$ genügen dem ersten, die Größen $\varrho, \varrho^3, \dots\ \varrho^{\ell-2}$ dem zweiten Faktor, sodaß vermöge ihrer symmetr. Grundfunktionen obige Gleichung als richtig erkannt wird. Damit wird also

$$h_1 = (-1)^{\frac{\ell-1}{2}} \frac{\ell^{\frac{\ell-1}{2}} (-1)^{\frac{\ell-1}{2}} g(\varrho) g(\varrho^3) \dots g(\varrho^{\ell-2})}{(2\ell)^{\frac{\ell-3}{2}} (-1)^{\frac{\ell-1}{2}} (r^{\frac{\ell-1}{2}} + 1)} \qquad \text{oder:}$$

I, 107

$$h_1 = (-1)^{\frac{\ell-1}{2}} \frac{\ell g(\varrho)g(\varrho^3)\dots g(\varrho^{\ell-2})}{2^{\frac{\ell-3}{2}}(r^{\frac{\ell-1}{2}}+1)}$$

Nun darf offenbar r so gewählt werden, daß

$$r^{\frac{\ell-1}{2}} \not\equiv 0 \mod \ell^2$$

ist, wozu ja $r^{\ell-1} \not\equiv 1 \mod \ell^2$ genügt. Dann ist der Nenner von h_1 genau durch ℓ teilbar, also gilt:

Satz 1: *Der erste Klassenzahlfaktor h_1 enthält den Faktor ℓ genau so oft, als er in dem Produkt $g(\varrho)g(\varrho^3)\dots g(\varrho^{\ell-2})$ aufgeht.*

Die Einheitswurzeln $\varrho, \varrho^3, \dots \varrho^{\ell-2}$ sind im Körper der ℓ–adischen Zahlen rational und mod. ℓ inkongruent, ferner, wenn $\varrho \equiv r$ mod. ℓ gewählt wird, was zulässig, kongruent $r, r^3, \dots r^{\ell-2}$ mod. ℓ. $g(\varrho^i)$ ist also dann und nur dann durch ℓ teilbar, wenn es $g(r^i)$ ist, und somit enthält h_1 den Faktor ℓ mindestens so oft, als es unter den Zahlen

$$g(r^i) = q_0 + q_1 r^i + q_2 r^{2i} + \dots + q_{\ell-2} r^{(\ell-2)i}$$

für $i = 1, 3, \dots, \ell-2$ durch ℓ teilbare gibt.

Wir haben nunmehr die Möglichkeit der Kongruenzen

$$g(r^{2t-1}) = q_0 + q_1 r^{2t-1} + \dots + q_{\ell-2} r^{(\ell-2)(2t-1)} \equiv 0 \mod \ell$$

für $t = 1, 2, \dots \frac{\ell-1}{2}$ zu untersuchen.

Nun ist

$$r r_\nu = r_{\nu+1} + (r r_\nu - r_{\nu+1}) = r_{\nu+1} + \ell q_\nu$$

also:

I, 108

$$\begin{aligned} (r r_\nu)^{2t} &\equiv r_{\nu+1}^{2t} + 2t\ell q_\nu r_{\nu+1}^{2t-1} \text{ mod. } \ell^2 \\ &\equiv r_{\nu+1}^{2t} + 2t\ell q_\nu r^{(\nu+1)(2t-1)} \text{ mod. } \ell^2 \end{aligned}$$

oder

$$2t\ell q_\nu r^{(\nu+1)(2t-1)} \equiv r^{2t} r_\nu^{2t} - r_{\nu+1}^{2t} \text{ mod. } \ell^2$$

also

$$\begin{aligned} 2t\ell r^{2t-1}\sum_{\nu=0}^{\ell-2} q_\nu r^{\nu(2t-1)} &= 2t\ell r^{2t-1} g(r^{2t-1}) \\ &\equiv r^{2t}\sum_{\nu=0}^{\ell-2} r_\nu^{2t} - \sum_{\nu=0}^{\ell-2} r_{\nu+1}^{2t} \text{ mod. } \ell^2 \\ &\equiv (r^{2t}-1)\left(1^{2t}+2^{2t}+\cdots+(\ell-1)^{2t}\right) \quad \text{mod } \ell^2 \end{aligned}$$

Also ist $g(r^{2t-1})$ ist also dann und nur dann durch ℓ teilbar, wenn

$$(r^{2t}-1)\left(1^{2t}+2^{2t}+\cdots+(\ell-1)^{2t}\right)$$

durch ℓ^2 teilbar ist. Nun ist $r^{2t}-1$ für $t=1,2,\dots\frac{\ell-3}{2}$ prim zu ℓ, für $t=\frac{\ell-1}{2}$ nach unserer Annahme genau einmal durch ℓ teilbar. Für $t=\frac{\ell-1}{2}$ ist ferner

$$1^{2t}+2^{2t}+\cdots(\ell-1)^{2t} \equiv -1 \quad \text{mod } \ell$$

also unser Ausdruck nicht durch ℓ^2 teilbar. Für $t=1,2,\dots\frac{\ell-3}{2}$ ist bekanntlich (symbolisch):

$$\begin{aligned} 1^{2t}+2^{2t}+\cdots+x^{2t} &= \frac{(x+\mathsf{B})^{2t+1}-\mathsf{B}^{2t+1}}{2t+1} \\ &= \frac{x^{2t+1}}{2t+1}+\sum_{\nu=1}^{2t}\binom{2t}{\nu-1}\frac{\mathsf{B}_\nu}{\nu}x^{2t+1-\nu} \end{aligned}$$

I, 109 wo die B_ν die Bernoullischen Zahlen in meiner Bezeichnungsweise bedeuten. Da die rechts auftretenden Nenner für $t=1,2,\dots\frac{\ell-3}{2}$ alle prim zu ℓ sind, und auch die Nenner der B_ν, die ja höchstens $(\nu+1)!$ sind, folgt für $x=\ell$:

$$1^{2t}+2^{2t}+\cdots+\ell^{2t} \equiv 1^{2t}+2^{2t}+\cdots+(\ell-1)^{2t} \equiv \mathsf{B}_{2t}\ell \quad \text{mod } \ell^2$$

$g(r^{2t-1})$ ist also für $t=1,2,\dots\frac{\ell-3}{2}$ dann und nur dann durch ℓ teilbar, wenn B_{2t} durch ℓ teilbar ist. Also gilt:

Satz 2. *Der erste Klassenzahlfaktor h_1 des Kreiskörpers k_ζ der ℓ–ten Einheitswurzeln enthält den Faktor ℓ dann und nur dann, wenn eine der ersten $\ell-3$ Bernoullischen Zahlen durch ℓ teilbar ist und zwar dann mindestens so oft, als es solche Bernoullischen Zahlen gibt.*

Bemerkung: Dabei ist natürlich von der Teilbarkeit der Bernoullischen Zahlen B_{2t+1} durch ℓ abzusehen. Besser muß man also sagen: „wenn eine der ersten

I, 110 $\frac{\ell-3}{2}$ Bernoullischen Zahlen $\neq 0$ durch ℓ teilbar ist“. Was gemeint ist, ist ja klar.

b.) Sätze über Einheiten in k_ζ.

Nach Seite 36] hat die Einheit $\varepsilon = -\frac{\lambda^{\ell-1}}{\ell}$ aus k_ζ durch die Takagische Basis die Darstellung:

$$\varepsilon \equiv k_1^{-\frac{1}{2}} k_2^{\frac{\mathsf{B}_2}{2\cdot 2!}} k_4^{\frac{\mathsf{B}_4}{4\cdot 4!}} \dots k_{\ell-3}^{\frac{\mathsf{B}_{\ell-3}}{(\ell-3)\cdot(\ell-3)!}} \mod \lambda^\ell$$

Vermöge der Eigenschaft

$$k_i^{s-r^i} \equiv 1 \mod \lambda^{\ell+1}$$

der k_i läßt sich daher durch symbolische Potenzierung aus ε ein System von Einheiten folgender Form herleiten:

$$\begin{array}{lll} \eta_2 \equiv 1 + \mathsf{B}_2\lambda^2 & \mod \lambda^3 \\ \eta_4 \equiv 1 + \mathsf{B}_4\lambda^4 & \mod \lambda^5 \\ \quad \dots\dots\dots\dots & \\ \eta_{\ell-3} \equiv 1 + \mathsf{B}_{\ell-3}\lambda^{\ell-3} & \mod \lambda^{\ell-2}. \end{array}$$

Es gilt ferner:

Satz 3. *Existiert in k_ζ eine Einheit des Typus $1+c\lambda^\kappa+\cdots$ mit zu ℓ primen c und $1 \leqq \kappa \leqq \ell-1$, so existiert in k_ζ sicher keine Einheit des Typus $1+c'\lambda^{\ell-\kappa}+\cdots$ mit zu ℓ primem c'.*

Beweis. Wären $\eta_\kappa, \eta_{\ell-\kappa}$ zwei solche, so wäre nach dem Reziprozitätsgesetz:

$$1 = \left(\frac{\eta_\kappa}{\eta_{\ell-\kappa}}\right)\left(\frac{\eta_{\ell-\kappa}}{\eta_\kappa}\right)^{-1} = \zeta^{-\kappa\, cc'},$$

was falsch ist. I, 111

Aus $\zeta = 1-\lambda$ folgt speziell:

Satz 4. *In k_ζ gibt es keine Einheit vom Typus $1+c\lambda^{\ell-1}+\cdots$ mit zu ℓ primem c.*

Aus $\left(\frac{\lambda}{1-\lambda^\ell}\right) = \zeta$ folgt ferner, daß auch keine Zahl der Form $1+c\lambda^\ell+\cdots$ Einheit sein kann:

Satz 5. *In k_ζ gibt es keine Einheit vom Typus $1+c\lambda^\ell+\cdots$ mit zu ℓ primem c.*

Liegt eine Einheit $\varepsilon = 1+c\lambda^\kappa+\cdots$ in k_ζ vor, so kann dieselbe nach S. 74] durch Multiplikation mit einer Potenz von ζ in eine reelle Einheit verwandelt werden. Diese Potenz ζ^{-g} ergibt sich nach S. 74] aus

$$\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} = +\zeta^{2g}$$

wo nach S. 74] sicher das + Zeichen steht. Das ergibt hier

$$\frac{1+c(1-\zeta)^\kappa+\cdots}{1+c(1-\zeta^{-1})^\kappa+\cdots} = \frac{1+c(1-\zeta)^\kappa+\cdots}{1+c\zeta^{-\kappa}(\zeta-1)^\kappa+\cdots}$$
$$= \frac{1+c\lambda^\kappa+\cdots}{1\pm c\lambda^\kappa+\cdots} = 1+(\lambda^\kappa)$$

Das kann aber für $\kappa > 1$ niemals ζ^{2g} werden, wenn nicht $g \equiv 0$ mod. ℓ, also $\zeta^{-g} = 1$ ist. Also:

I, 112 **Satz 6:** *Jede Einheit vom Typus* $1 + c\lambda^\kappa + \cdots$ *für* $\kappa > 1$ *ist notwendig reell.*

Ist ε eine beliebige Einheit aus k_ζ, so ist $\varepsilon^{\ell-1} \equiv 1 \mod \lambda$. Stellt man dann $\varepsilon^{\ell-1}$ durch die Takagische Basis dar:

$$\varepsilon^{\ell-1} \equiv k_1^{c_1} k_2^{c_2} \ldots k_\ell^{c_\ell} \mod \lambda^{\ell+1}$$

so folgt aus $k_1 = \zeta$ und der Eindeutigkeit des oben genannten ζ^{-g}, daß $\varepsilon^{\ell-1}\zeta^{-c_1}$ reell ist. Ich setze

$$\eta = \varepsilon^{\ell-1}\zeta^{-c_1} \equiv k_2^{c_2} k_3^{c_3} \cdots k_\ell^{c_\ell} \text{ mod. } \lambda^{\ell+1}$$

Wäre nun einer der Exponenten $c_3, c_5, \ldots c_{\ell-2}, c_{\ell-1}, c_\ell \mod \ell$ von Null verschieden, so würde durch Erheben in eine passende symbolische Potenz eine Einheit vom Typus

$$\overline{\eta} = 1 - c_i\lambda^i + \cdots$$

folgen, wo i einer der Indizes $3, 5, \ldots, \ell-2, \ell-1, \ell$ ist. Für $i = \ell-1, \ell$ folgt aus Satz 4,5 ein Widerspruch, für $i = 3, 5, \ldots, \ell-2$ aus Satz 6. Letzterer besagt nämlich offenbar, *daß Einheiten vom Typus* $1{+}c\lambda^{2\kappa+1}$ *für* $\kappa \geqq 1$ *mit zu* ℓ *primem* c *überhaupt nicht existieren können.* Denn nach ihm läßt sich jede solche Einheit eindeutig nach Potenzen von $\overline{\lambda} = (1-\zeta)(1-\zeta^{-1}) = -\zeta^{-1}\lambda^2$ entwickeln, muß also so beginnen:

$$1 + c\overline{\lambda}^\kappa + \cdots = 1 - c\zeta^{-1}\lambda^{2\kappa} + \cdots = 1 - c\lambda^{2\kappa} + \cdots .$$

I, 113 Damit ist folgender Satz bewiesen: **Satz 7.** *Jede Einheit* ε *aus* k_ζ *gestattet eine Darstellung folgender Art durch die Takagische Basis:*

$$\varepsilon \equiv \varepsilon^\ell k_1^{c_1} k_2^{c_2} k_4^{c_4} \ldots k_{\ell-3}^{c_{\ell-3}} \mod \lambda^{\ell+1}.$$

c.) Der zweite Klassenzahlfaktor.

Der zweite Faktor der Klassenzahl ist nach Satz 3, S. 76]:

$$h_2 = \frac{(-1)^{\frac{\ell-3}{2}}\mathsf{P}}{\mathsf{R}}$$

Dabei ist P eine Determinante, die aus der Kreiseinheit

$$\varepsilon_0 = \sqrt{\frac{(1-\zeta)(1-\zeta^{-1})}{(1-\zeta^{r^{-1}})(1-\zeta^{-r^{-1}})}} \qquad \text{(Wurzel positiv!)}$$

entspringt (Siehe S. 73]). Bezeichnet $s = (\zeta : \zeta^r)$ die erzeugende Substitution von k_ζ, so ist wegen $s^{\frac{\ell-1}{2}} = (\zeta : \zeta^{-1})$ das System von Substitutionen

$$1, s, s^2, \dots s^{\frac{\ell-3}{2}}$$

so beschaffen, daß es aus α gerade von jedem Paar konjugiert–komplexer konjugierter eine erzeugt, ebenso auch $1, s^{-1}, s^{-2}, \dots, s^{-\frac{\ell-3}{2}}$. Nun läßt sich die Determinante P wegen $\varepsilon_\nu = s^\nu \varepsilon_0$, $\varepsilon_\nu = \varepsilon_{\nu'}$ wenn $\nu \equiv \nu' \mod \frac{\ell-1}{2}$ so schreiben:

$$\mathsf{P} = \begin{vmatrix} \log \varepsilon_0 & \log s\varepsilon_0 & \cdots\cdots & \log s^{\frac{\ell-5}{2}}\varepsilon_0 \\ \log s^{-1}\varepsilon_0 & \log s^{-1}s\varepsilon_0 & \cdots\cdots & \log s^{-1}s^{\frac{\ell-5}{2}}\varepsilon_0 \\ & & & \\ \log s^{-\frac{\ell-5}{2}}\varepsilon_0 & \log s^{-\frac{\ell-5}{2}}s\varepsilon_0 & \cdots\cdots & \log s^{-\frac{\ell-5}{2}}s^{\frac{\ell-5}{2}}\varepsilon_0 \end{vmatrix}$$
$$\big(\log = \text{Hauptwert!}\big)$$

I, 114

Diese Form von P läßt erkennen, daß P gerade diejenige Determinante ist, deren Verschwinden über die Abhängigkeit der $\frac{\ell-3}{2}$ Einheiten

$$\varepsilon_0, s\varepsilon_0, \dots, s^{\frac{\ell-5}{2}}\varepsilon_0$$

entscheidet. Wegen $h_2 \neq 0$ ist $\mathsf{P} \neq 0$, also:

Satz 8. *Die $\frac{\ell-3}{2}$ Kreiseinheiten $\varepsilon_0, s\varepsilon_0, \dots, s^{\frac{\ell-5}{2}}\varepsilon_0$, wo ε_0 die positive Quadratwurzel aus der reell–positiven Einheit*

$$\frac{(1-\zeta)(1-\zeta^{-1})}{(1-\zeta^{r^{-1}})(1-\zeta^{-r^{-1}})}$$

ist, die in k_ζ stets aufgeht, sind von einander unabhängig.

Bemerkung: Daraus folgt natürlich leicht, daß auch die durch dieselben Substitutionen aus

$$\varepsilon_1 = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}}$$

entstehenden $\frac{\ell-3}{2}$ Einheiten unabhängig sind, denn hier fällt ε_0 weg, während $\varepsilon_{\frac{\ell-3}{2}}$ neu hinzukommt. Es ist aber

$$\varepsilon_0\varepsilon_1\ldots\varepsilon_{\frac{\ell-3}{2}} = \varepsilon_0^{1+s+\cdots+s^{\frac{\ell-3}{2}}} = \varepsilon_0^{\frac{s^{\frac{\ell-1}{2}}-1}{s-1}}$$

und da s in Bezug auf ε_0 der Gleichung $s^{\frac{\ell-1}{2}} = 1$ genügt ist dies $= 1$, was auch daraus erschlossen werden kann, daß dieses Produkt die Norm der reellen Einheit ε_0 im Unterkörper der zweigliedrigen Perioden ist. Es darf somit unbeschadet der Unabhängigkeit ε_0 durch $\varepsilon_{\frac{\ell-3}{2}}$ ersetzt werden. Es sei nun im folgenden

I, 115

$$n = \frac{\ell-3}{2}\,.$$

Ferner sei $\gamma_1, \gamma_2, \ldots \gamma_n$ ein System von (reellen) Grundeinheiten von k_ζ. Dann kann

$$s^{i-1}\varepsilon_0 = \prod_{\kappa=1}^{n} |\gamma_\kappa|^{m_{i\kappa}}\ ; \quad (i = 1, 2, \ldots n) \tag{1}$$

gesetzt werden mit ganzen rationalen $m_{i\kappa}$. Ferner ziehen wir die a. S. 110] konstruierten Einheiten

$$\eta_2, \eta_4, \ldots, \eta_{\ell-3}\,,$$

deren Anzahl ebenfalls n ist, hinzu. Diese entstehen sämtlich durch symbolische Potenzierung von

$$\varepsilon = -\frac{\lambda^{\ell-1}}{\ell}$$

Nun ist

$$\begin{aligned}
\varepsilon &= -\frac{\lambda^{\ell-1}}{\ell} = -\prod_{\nu=0}^{\ell-2}\frac{1-\zeta}{1-\zeta^{r^\nu}} = +\zeta\prod_{\nu=0}^{\frac{\ell-3}{2}}\frac{(1-\zeta)(1-\zeta^{-1})}{(1-\zeta^{r^\nu})(1-\zeta^{-r^\nu})}\\
&= +\zeta\prod_{\nu=0}^{\frac{\ell-3}{2}}\varepsilon_1^{-2}\cdot s\varepsilon_1^{-2}\cdots s^{\nu-1}\varepsilon_1^{-2} = +\zeta\prod_{\nu=0}^{\frac{\ell-3}{2}}\varepsilon_1^{-2(1+s+\cdots+s^{\nu-1})}\\
&= +\zeta\varepsilon_1^{-2\sum_{\nu=0}^{\frac{\ell-3}{2}}(1+s+\cdots+s^{\nu-1})} = +\zeta\varepsilon_1^{\overline{f}(s)}
\end{aligned}$$

und da $\varepsilon_1 = \varepsilon_0^s$ auch

$$\varepsilon = +\zeta\,\varepsilon_0^{f(s)}$$

Daraus folgt, daß ε und auch jede symbolische Potenz von ε sich als symbolische Potenz von ε_0 darstellen läßt, bis auf eine ev. Einheitswurzel. Da die Einheiten $\eta_2, \eta_4, \ldots, \eta_{\ell-3}$ nach Satz 6 reell sind, fällt diese Einheitswurzel bei der symbolischen Potenzierung heraus, was natürlich auch daraus folgt, daß ε um k_1 zum Wegfall zu bringen mit $s-r$ potenziert werden muß. I, 116

Es sind also $\eta_2, \eta_4, \ldots\ \eta_{\ell-3}$ symbolische Potenzen von ε_0 also durch die unabhängigen unter diesen symbolischen Potenzen, nämlich $\varepsilon_0, s\varepsilon_0, \ldots\ s^{n-1}\varepsilon_0$ in der Form darstellbar:

$$\eta_{2i} = \prod_{\kappa=1}^{n}\left(s^{\kappa-1}\varepsilon_0\right)^{n_{i\kappa}}\ ; \quad (i = 1, 2, \ldots\ n) \tag{2}$$

(wobei ersichtlich der absolute Betrag *nicht* genommen zu werden braucht, weil die η_{2i} als symbolische Potenzen von $\varepsilon^{s-r} = \varepsilon_0^{(s-r)f(s)}$ positiv sind, weil ε_0 total positiv ist!).

Aus (1) und (2) folgt

$$\eta_{2i} = \prod_{\kappa=1}^{n}|\gamma_\kappa|^{\mathsf{M}_{i\kappa}}\ ; \quad (i = 1, 2, \ldots\ n) \tag{3}$$

wenn

$$(\mathsf{M}_{i\kappa}) = (n_{i\kappa})(m_{i\kappa})$$

das Matrizenprodukt der beiden Substitutionsmatrizen ist. Bezeichnen ferner R, E, H die aus den Logarithmen der $|\gamma_\kappa|$, $s^{\kappa-1}\varepsilon_0$, $\eta_{2\kappa}$ und ihren konjugierten gebildeten Determinanten ihrem absoluten Betrage nach, so gilt wenn noch M, N,

M die Substitutionsdeterminanten von (1), (2), (3) bezeichnen (ebenfalls ihrem
I, 117 Betrage nach):

$$\left.\begin{array}{rcl}\mathsf{E} &=& M\mathsf{R},\\ \mathsf{H} &=& N\mathsf{E} = \mathsf{MR},\end{array}\right\}\mathsf{M} = MN$$

also

$$\frac{\mathsf{H}}{\mathsf{R}} = \frac{\mathsf{H}}{\mathsf{E}}\cdot\frac{\mathsf{E}}{\mathsf{R}} = \mathsf{M}\,.$$

Der zweite Faktor $\frac{\mathsf{E}}{\mathsf{R}}$ ist wegen der Bedeutung von $\mathsf{E} = |\mathsf{P}|$ ersichtlich gleich h_2, sodaß wegen $\frac{\mathsf{H}}{\mathsf{E}} = N$

$$N\,h_2 = \mathsf{M}$$

resultiert. Die Determinante N ist eine ganze reationale Zahl. h_2 wird also sicher dann prim zu ℓ, wenn die ganze Zahl M es ist.

Ich zeige nun, daß M, d. h. die den n „Bernoullischen Einheiten“

$$\begin{array}{lcl}\eta_2 &=& 1 + \mathsf{B}_2\lambda^2 + \cdots\\ \eta_4 &=& 1 + \mathsf{B}_4\lambda^4 + \cdots\\ \cdots && \cdots\cdots\cdots\cdots\cdots\\ \eta_{\ell-3} &=& 1 + \mathsf{B}_{\ell-3}\lambda^{\ell-3} + \cdots\end{array}$$

in Bezug auf die Grundeinheiten entsprechende Substitual–Determinante sicher dann prim zu ℓ, also speziell auch von Null verschieden ist, wenn jene Bernoullischen Zahlen sämtlich prim zu ℓ sind.

Wäre nämlich M durch ℓ teilbar, so gäbe es n ganze rationale nicht sämtlich durch ℓ teilbare Zahlen $\mathsf{N}_1, \ldots, \mathsf{N}_n$ sodaß

$$(i,\kappa\ \textit{vertauscht!})\qquad \sum_{\kappa=1}^{n}\mathsf{N}_\kappa\mathsf{M}_{\kappa i} \equiv 0 \mod. \ell\,;\quad (i = 1, 2, \ldots n)$$

I, 118 wäre, also nach (3):

$$\prod_{i=1}^{n}\eta_{2i}^{\mathsf{N}_i} = \prod_{\kappa=1}^{n}|\gamma_\kappa|^{\sum_{i=1}^{n}\mathsf{N}_i\mathsf{M}_{i\kappa}} = \eta^\ell$$

die ℓ–te Potenz einer (reellen, positiven) Einheit η wäre. Dies ist aber auf Grund der gemachten Voraussetzung über die Bernoullischen Zahlen unmöglich, da dann die $\eta_2, \eta_4, \ldots, \eta_{\ell-3}$ unabhängige Nichtreste mod $\lambda^{\ell+1}$ sind.

Damit ist bewiesen, daß wenn h_1 prim zu ℓ ist, auch h_2 es ist, also:

Satz 9. *Dann und nur dann, wenn die sämtlichen Bernoullischen Zahlen* $\mathsf{B}_2, \mathsf{B}_4, \ldots, \mathsf{B}_{\ell-3}$ *prim zu* ℓ *sind, ist die Klassenzahl von* k_ζ *prim zu* ℓ.

Außerdem nach der letzten Bemerkung:

Satz 10. *Die* $n = \frac{\ell-3}{2}$ *„Bernoullischen Einheiten" des regulären Kreiskörpers sind unabhängig.*

1.12 Einige Ergänzungen zu meiner Vorlesung: Galoissche Theorie (11.10.1923)

Some direct consequences of the Main Theorem of Galois Theory which Hasse did not cover in his lecture course. In the winter semester 1923/24 Hasse, being "Privatdozent" in Kiel, gave a course "Algebra II" (4 hours weekly).

I, 119

11. X. 23.

Es sei $\Omega(\varrho)$ Normalkörper über Ω, $\mathfrak{G}$ die Gruppe der Automorphismen von $\Omega(\varrho)$ über Ω (Galoissche Gruppe von $\Omega(\varrho)$ nach Ω). Dann besteht der Satz von der umkehrbar eindeutigen Zuordnung der Unterkörper $\Omega(\eta)$ von $\Omega(\varrho)$ über Ω zu den Untergruppen $\mathfrak{H}$ von $\mathfrak{G}$.

Hauptsatz. Jedem Unterkörper $\Omega(\eta)$ entspricht eindeutig eine Untergruppe $\mathfrak{H}$, nämlich die Gesamtheit aller Automorphismen, die $\Omega(\eta)$ invariant lassen; Zeichen: $\Omega(\eta) \longrightarrow \mathfrak{H}$.

Jeder Untergruppe $\mathfrak{H}$ entspricht eindeutig ein Unterkörper $\Omega(\eta)$, nämlich die Gesamtheit aller Elemente von $\Omega(\varrho)$, die bei $\mathfrak{H}$ invariant bleiben; Zeichen $\mathfrak{H} \longrightarrow \Omega(\eta)$.

Wenn $\Omega(\eta) \longrightarrow \mathfrak{H}$ ist $\mathfrak{H} \longrightarrow \Omega(\eta)$ und umgekehrt, also kann

$$\Omega(\eta) \longleftrightarrow \mathfrak{H}$$

geschrieben werden.

Es gelten ferner folgende Ergänzungen:

I. Ist $\mathfrak{H}_1 \longleftrightarrow \Omega(\eta_1)$, $\mathfrak{H}_2 \longleftrightarrow \Omega(\eta_2)$ und

$$\mathfrak{H}_1 \mid \mathfrak{H}_2 \quad \text{vom Index } i,$$

so ist $\Omega(\eta_1) > \Omega(\eta_2)$ vom Relativgrad i und umgekehrt. Speziell ist

$$\Omega \longleftrightarrow \mathfrak{G}\,, \quad \Omega(\varrho) \longleftrightarrow \mathfrak{E}.$$

I, 120

Ist also n der Grad von $\mathfrak{G}$, und

$$\mathfrak{H} \longleftrightarrow \Omega(\eta)$$

so ist der Grad ν von $\Omega(\varrho)$ über $\Omega(\eta)$ gleich dem Grad von $\mathfrak{H}$, der Grad $\mathfrak{j}$ von $\Omega(\eta)$ über Ω gleich dem Index von $\mathfrak{H}$, und $n\nu = \mathfrak{j}$.

II. Ist $\mathfrak{H} \longleftrightarrow \Omega(\eta)$, so ist $\mathfrak{H}$ die Galoissche Gruppe von $\Omega(\varrho)$ nach $\Omega(\eta)$ und $\mathfrak{G}/\mathfrak{H}$ die Galoissche Gruppe von $\Omega(\eta)$ nach Ω.

III. Ist $\mathfrak{H}_1 \longleftrightarrow \Omega(\eta_1)$, $\mathfrak{H}_2 \longleftrightarrow \Omega(\eta_2), \dots$ so ist der Durchschnitt

$$(\mathfrak{H}_1, \mathfrak{H}_2, \dots) = \mathfrak{D} \longleftrightarrow \Omega(\eta_1, \eta_2, \dots) = \big(\Omega(\eta_1), \Omega(\eta_2) \dots\big)$$

d. h. dem komponierten Körper zugeordnet und umgekehrt.

IV. Ist $\mathfrak{H}$ Normalteiler, so ist $\Omega(\eta)$ Normalkörper und umgekehrt.

Diese Sätze sind in meiner Vorlesung bewiesen.
Es gilt überdies:

V. Ist $\mathfrak{H}_1 \longleftrightarrow \Omega(\eta_1)$, $\mathfrak{H}_2 \longleftrightarrow \Omega(\eta_2), \dots$, so ist die „Vereinigungsgruppe“ (mit allen Produktreihenfolgen):

$$\big\{\mathfrak{H}_1, \mathfrak{H}_2, \dots\big\} = \mathfrak{V} \longleftrightarrow \big\{\Omega(\eta_1), \Omega(\eta_2), \dots\big\} = \Omega(\delta)$$

dem Durchschnitt der Körper.

Beweis: 1.) jedes Element von $\Omega(\delta)$ bleibt bei allen Automorphismen von $\mathfrak{H}_1, \mathfrak{H}_2, \dots$, also bei allen von $\mathfrak{V}$ invariant.
2.) Jedes Element von $\Omega(\varrho)$, das bei allen $\mathfrak{H}_1, \mathfrak{H}_2, \dots$ invariant bleibt, gehört zu jedem $\Omega(\eta_1), \Omega(\eta_2)$, also zu $\Omega(\delta)$. I, 121

Es seien jetzt speziell die $\mathfrak{H}_i$ zu je zweien teilerfremd und untereinander elementweise vertauschbar. Dann ist also der Durchschnitt $\mathfrak{D} = \mathfrak{E}$ und es existiert das direkte Produkt

$$\mathfrak{V} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots = \big\{\mathfrak{H}_1, \mathfrak{H}_2, \dots\big\}.$$

Dann gilt nach III.:

$$\Omega(\eta_1, \eta_2, \dots) \longleftrightarrow (\mathfrak{H}_1, \mathfrak{H}_2, \dots) = \mathfrak{E} \longleftrightarrow \Omega(\varrho)$$

also

$$\Omega(\eta_1, \eta_2, \dots) = \Omega(\varrho).$$

VI. Ist $\mathfrak{H}_1 \longleftrightarrow \Omega(\eta_1)$, $\mathfrak{H}_2 \longleftrightarrow \Omega(\eta_2), \dots$ und sind die $\mathfrak{H}_i$ teilerfremd, so ist $\Omega(\varrho)$ aus den $\Omega(\eta_i)$ komponiert. Sind überdies die $\mathfrak{H}_i$ elementweise vertauschbar und zu je zweien teilerfremd, so ist nach V.,II. ihr direktes Produkt die Galoissche Gruppe von $\Omega(\varrho)$ nach $\Omega(\delta)$. Sind also speziell die $\Omega(\eta_i)$ teilerfremd, so folgt:

$$\mathfrak{G} = \mathfrak{H}_1 \times \mathfrak{H}_2 \times \cdots$$

Es seien nun $\Omega(\eta_1)$, $\Omega(\eta_2)$, ... eine Reihe von Normalkörpern über Ω und $\Omega(\delta) = \Omega$, d. h. diese Körper teilerfremd, ferner $\Omega(\eta_1, \eta_2, \dots) = \Omega(\varrho)$, sodaß auch $\Omega(\varrho)$ Normalkörper. $\mathfrak{G}$ sei die Gruppe von $\Omega(\varrho)$ und $\mathfrak{H}_i \longleftrightarrow \Omega(\eta_i)$. Dann ist

1.) $(\mathfrak{H}_1, \mathfrak{H}_2, \dots) = \mathfrak{E}$, weil $\Omega(\varrho)$ zugeordnet.

2.) $\{\mathfrak{H}_1, \mathfrak{H}_2, \dots\} = \mathfrak{G}$, weil Ω zugeordnet.

I, 122 Wir bilden die Gruppen

$$\mathfrak{K}_1 = (\mathfrak{H}_2, \dots), \mathfrak{K}_2, \dots ,$$

sodaß $\mathfrak{K}_i$ gleich der Gesamtheit der Automorphismen, die höchstens η_i ändern. Es ist dann nach III.

$$\begin{array}{lll} & \mathfrak{K}_1 \longleftrightarrow \Omega(\eta_2, \dots) & \\ & \dots\dots\dots\dots\dots\dots & \\ \text{Ferner} & (\mathfrak{K}_1, \mathfrak{K}_2) = \dots = \mathfrak{E} & \quad \text{nach 1.)} \\ & \{\mathfrak{K}_1, \mathfrak{K}_2, \dots\} = \mathfrak{G} & \end{array}$$

letzteres, weil der Durchschnitt

$$\{\Omega(\eta_2, \eta_3 \dots), \Omega(\eta_1, \eta_3, \dots), \dots\} = \Omega$$

ist. Schließlich sind $\mathfrak{K}_1, \mathfrak{K}_2, \dots$ elementweise vertauschbar. Denn ist

$$\varrho = \chi(\eta_1, \eta_2, \dots)$$

so ist für k_1 aus $\mathfrak{K}_1$, k_2 aus $\mathfrak{K}_2$:

$$\begin{aligned} \varrho/k_1 &= \chi(\eta_1/k_1, \eta_2, \dots) \\ \varrho/k_2 &= \chi(\eta_1, \eta_2/k_2, \dots) \end{aligned}$$

also

$$\varrho/k_1k_2 = \varrho/k_2k_1 = \chi(\eta_1/k_1, \eta_2/k_2, \eta_3, \dots)$$

Daher ist

$$\mathfrak{G} = \mathfrak{K}_1 \times \mathfrak{K}_2 \times \cdots .$$

Nun ist dem direkten Produkt $\mathfrak{K}_2 \times \mathfrak{K}_3 \times \cdots$ der Durchschnitt $\{\Omega(\eta_1, \eta_3, \dots), \Omega(\eta_1, \eta_2, \eta_4 \dots), \dots\}$ zugeordnet. Dieser Durchschnitt ist sicher Oberkörper von $\Omega(\eta_1)$, würde er aber noch einen Teilkörper von $\Omega(\eta_2, \eta_3, \dots)$ enthalten, so wären

die Körper $\Omega(\eta_2), \Omega(\eta_3), \dots$ nicht prim zu $\Omega(\eta_1)$. Wir setzen daher voraus, daß unser Körper $\Omega(\eta_i)$ zu je zweien relativ prim, d. h. jeder prim zum Kompositum der übrigen ist. Dann folgt: I, 123

$$\mathfrak{K}_2 \times \mathfrak{K}_3 \times \cdots \longleftrightarrow \Omega(\eta_1) \longleftrightarrow \mathfrak{H}_1$$

Also ist $\mathfrak{K}_1$ als Faktorgruppe $\mathfrak{G}/\mathfrak{K}_2 \times \mathfrak{K}_3 \times \cdots$ die Galoissche Gruppe von $\Omega(\eta_1)$, u. s. w.

Damit ist bewiesen

VII. Sind die Normalkörper $\Omega(\eta_1), \Omega(\eta_2), \dots$ zu je zweien relativ prim, d. h. keiner im Kompositum der übrigen enthalten, so ist die Galoissche Gruppe $\mathfrak{G}$ des Kompositums

$$\Omega(\varrho) = \Omega(\eta_1, \eta_2, \dots)$$

das direkte Produkt

$$\mathfrak{G} = \mathfrak{K}_1 \times \mathfrak{K}_2 \times \cdots$$

Dabei bedeuten $\mathfrak{K}_1, \mathfrak{K}_2, \dots$ diejenigen Automorphismen von $\Omega(\varrho)$, die höchstens $\eta_1, \eta_2, \dots$ ändern, und diese Faktoren $\mathfrak{K}_i$ sind mit den Galoisschen Gruppen der $\Omega(\eta_i)$ isomorph.

1.13 Ansatz zur analytischen Behandlung des Fermatschen Satzes. (15.11.1923)

Hasse transforms Fermat's Last Theorem via Cauchy's integral formula and Dirichlet summation into an analytic statement. In the winter semester 1923/24 Hasse, Steinitz and Toeplitz conducted a joint seminar with the title "Grenzgebiete von Zahlen- und Funktionentheorie". The topic of this entry seems to fit in this scheme. Maybe Hasse talked about it in the seminar, or he had a student give a talk about it.

I, 124

(Kiel, 15. XI. 1923.)

Die Reihe

$$\sum_{n=1}^{\infty} x^{n^\ell}$$

wo ℓ eine ungerade Primzahl ist, ist für $|x| < 1$ konvergent. Ich setze

$$x = e^{-\sigma} z\,; \quad \sigma > 0\,.$$

Dann folgt die Konvergenz von

$$\sum_{n=1}^{\infty} e^{-\sigma n^\ell} z^{n^\ell} \quad \text{für} \quad |z| < e^{\sigma}$$

und

$$\sum_{n=-1}^{-\infty} e^{-\sigma |n|^\ell} z^{n^\ell} \quad \text{für} \quad |z| > e^{-\sigma}$$

also von

$$f(\sigma, z) = \sum_{n=-\infty}^{+\infty} n^{\ell-1} e^{-\sigma |n|^\ell} z^{n^\ell} \quad \text{für} \quad e^{-\sigma} < |z| < e^{\sigma}$$

Der Koeffizient von z^0 in der ebendort konvergenten Laurentschen Reihe $f^3(\sigma, z)$ ist

$$\sum_{n^\ell + n'^\ell + n''^\ell = 0} (nn'n'')^{\ell-1} e^{-\sigma\{|n|^\ell + |n'|^\ell + |n''|^\ell\}}$$

Wenn der Fermatsche Satz richtig ist, muß dieser Ausdruck für alle $\sigma > 0$ verschwinden. Der fragliche Koeffizient berechnet sich nach den Cauchyschen Integralformeln auch so: I, 125

$$\frac{1}{2\pi i}\int\limits_{\mathsf{E}} f^3(\sigma, z)\,\frac{dz}{z}$$

erstreckt über den Einheitskreis E. Wir setzen daher

$$\begin{aligned} z &= e^{it} \\ \frac{dz}{z} &= i\,dt \end{aligned}$$

Dann muß

$$\int\limits_{-\pi}^{+\pi} f^3(\sigma, e^{it})\,dt = 0\,, \quad \text{für } \sigma > 0$$

nachgewiesen werden.

Nun ist

$$f(\sigma, e^{it}) = \sum_{n=-\infty}^{+\infty} n^{\ell-1} e^{-\sigma|n|^\ell + itn^\ell},$$

also nach der Dirichletschen Summenformel (S. 13] des Hefts):

$$f(\sigma, e^{it}) = \sum_{m=-\infty}^{+\infty}\ \int\limits_{-\infty}^{+\infty} u^{\ell-1} e^{-\sigma|u|^\ell + itu^\ell - 2\pi imu} du,$$

also

$$f^3(\sigma, e^{it}) = \sum_{m,m',m''} \iiint\limits_{u\ u'u''} (uu'u'')^{\ell-1}\cdot$$
$$\cdot\, e^{-\sigma\{|u|^\ell + |u'|^\ell + |u''|^\ell\} + it(u^\ell + u'^\ell + u''^\ell) - 2\pi i(mu + m'u' + m''u'')}\ du\,du'\,du''$$

wo Summation u. Integrationen, wie stets im folgenden von $-\infty$ bis $+\infty$ erstreckt werden.

Durch Einführung von $u^\ell = v$, $u'^\ell = v'$, $u''^\ell = v''$ wird noch: I, 126

$$f^3(\sigma, e^{it}) = \sum_{m,m',m''} \frac{1}{\ell^3} \iiint\limits_{v\ v'v''}$$
$$e^{-\sigma(|v| + |v'| + |v''|) + it(v + v' + v'') - 2\pi i(mv^{\frac{1}{\ell}} + m'v'^{\frac{1}{\ell}} + m''v''^{\frac{1}{\ell}})}\ dv\,dv'\,dv''$$

wobei $v^{\frac{1}{\ell}}, \ldots$ stets die reellen Werte bedeuten. Der fragliche Koeffizient wird also bis auf konstante Faktoren

$$\sum_{m,m',m''} \int_{\mathsf{V}} e^{-\sigma(|v|+|v'|+|v''|)-2\pi i(mv^{\frac{1}{\ell}}+m'v'^{\frac{1}{\ell}}+m''v''^{\frac{1}{\ell}})} \cdot \frac{\sin\pi(v+v'+v'')}{v+v'+v''}\, d\mathsf{V}$$

wenn $d\mathsf{V}$ das Volumenelement des V Raumes bezeichnet, der durch v, v', v'' bestimmt ist.

Alles kommt darauf an, das Verschwinden der letzten Integralsumme nachzuweisen.

1.14 Kettenbruchtheorie. (Nov. 1923)

Basic arithmetic of periodic continued fractions. Throughout his life Hasse was interested in continued fractions as algorithms for the computation of units in real quadratic number fields.

I, 127

(November 1923)

a.) Grundlagen

Sei $a_1, a_2, a_3, \dots$ eine endliche oder unendliche Folge von *positiven*, ganzen Zahlen, dann heißt:

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}}$$

ein Kettenbruch, die Zahlen seine *Nenner*.

Satz 1. Jeder Kettenbruch konvergiert gegen eine reelle Zahl α. Es ist

$$0 < \alpha \leqq 1$$

und dann und nur dann $\alpha = 1$, wenn $a_1 = 1$ alle folgenden $a_i = 0$ (nicht vorhanden).

Beweis. Wir betrachten die „*Näherungswerte*":

$$\alpha_n = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}} \quad ; \quad (n \geqq 1)$$

Deren erste sind

$$\alpha_1 = \frac{1}{a_1}\,, \ \alpha_2 = \frac{a_2}{a_1 a_2 + 1}\,, \ \dots$$

Setzen wir diese in der Form

$$\alpha_n = \frac{p_n}{q_n}$$

an, wo p_n und q_n die sich bei der Berechnung ergebenden Ausdrücke in Zähler und Nenner sind, die für *unbestimmte* a_i keine Kürzung mehr erlauben, setzen I, 128

wir ferner der Vollständigkeit halber

$$p_{-1} = 1\,; \qquad p_0 = 0$$
$$q_{-1} = 0\,; \qquad q_0 = 1$$

so gilt allgemein:

$$(1) \qquad \left.\begin{aligned} p_{n+1} &= a_{n+1}p_n + p_{n-1} \\ q_{n+1} &= a_{n+1}q_n + q_{n-1} \end{aligned}\right\} \text{ für } n \geqq 0.$$

Diese Rekursionsformeln stimmen nämlich nach dem obigen für $n = 0, 1$. Seien sie bis $n-1$ bewiesen, dann betrachten wir α_{n+1}, das aus α_n dadurch entsteht, daß a_n durch $a_n + \frac{1}{a_{n+1}}$ ersetzt wird.

Es wird dann also

$$\alpha_{n+1} = \frac{\left(a_n + \frac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \frac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}}\ ,$$

da p_{n-1}, q_{n-1}, p_{n-2}, q_{n-2} von a_n unabhängig sind. Also:

$$\alpha_{n+1} = \frac{a_{n+1}(a_n p_{n-1} + p_{n-2}) + p_{n-1}}{a_{n+1}(a_n q_{n-1} + q_{n-2}) + q_{n-1}} = \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}\ ,$$

und da letzterer Bruch für unbestimmtes a_{n+1} nicht weiter zu kürzen ist, weil p_n, q_n; p_{n-1}, q_{n-1} keinen Faktor gemeinsam haben sollen (nach Voraussetzung), wird

$$\begin{aligned} p_{n+1} &= a_{n+1}p_n + p_{n-1} \\ q_{n+1} &= a_{n+1}q_n + q_{n-1}\,, \end{aligned} \qquad \text{w. z. b. w.}$$

I, 129 Aus den damit bewiesenen Rekursionsformeln für die Zähler und Nenner der Näherungsbrüche α_n folgt weiter:

$$\Delta_n = \begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = \begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = - \begin{vmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{vmatrix} = -\Delta_{n-1}$$

also wegen

$$\Delta_0 = \begin{vmatrix} 0 & 1 \\ 1 & a_1 \end{vmatrix} = -1$$

allgemein

$$\Delta_n = (-1)^{n+1}$$

Daher sind stets p_n, q_n auch für irgendwelche numerischen a_i prim zu einander, und es ist $\alpha_n = \frac{p_n}{q_n}$ stets die reduzierte Darstellung

(Berechnung nach dem Schema

		a_1	a_2	a_3	$\cdots\cdots$
1	0	1	a_2	$\cdots$	$\cdots\cdots$
0	1	a_1	a_1a_2+1	$\cdots$	$\cdots\cdots$

)

Ferner folgt:

$$\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{\Delta_n}{q_n q_{n+1}} = \frac{(-1)^{n+1}}{q_n q_{n+1}}$$

Ist die Folge a_i also unendlich, so wächst nach den Rekursionsformeln q_n mit n über alle Grenzen, und die Folge $\alpha_n = \frac{p_n}{q_n}$ oszilliert daher in zu Null strebenden Schranken, nähert sich somit einer endlichen Grenze α, die auch als

$$\begin{aligned} \alpha &= \lim_{n=\infty} \frac{p_n}{q_n} = \lim_{n=\infty} \sum_{\nu=1}^{n} \left(\frac{p_\nu}{q_\nu} - \frac{p_{\nu-1}}{q_{\nu-1}} \right) = \lim_{n=\infty} \sum_{\nu=1}^{n} \frac{(-1)^{\nu+1}}{q_\nu q_{\nu-1}} \\ &= \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu+1}}{q_\nu q_{\nu-1}} = \frac{1}{q_1} - \frac{1}{q_2 q_1} + \frac{1}{q_3 q_2} - \frac{1}{q_4 q_3} + \cdots \end{aligned}$$

geschrieben werden kann. I, 130

Für den Grad der Annäherung der Näherungsbrüche $\alpha_n = \frac{p_n}{q_n}$ an α ergibt sich noch, da α stets zwischen zwei aufeinanderfolgenden liegt:

$$|\alpha - \alpha_n| < \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2} \,, \tag{2}$$

weil stets $q_{n+1} > q_n$, (wenn der Kettenbruch unendlich).

Natürlich ist für $a_1 = 1$, alle übrigen $a_i = 0$ $\alpha = 1$. Ist dies aber nicht der Fall, so ist entweder $a_1 > 1$, $a_i = 0$ und $0 < \alpha = \dfrac{1}{a_1} < 1$, oder α liegt im Intervall

$$0 < \frac{1}{a_1} \leqq \alpha \leqq \frac{a_2}{a_1 a_2 + 1} < 1$$

Damit ist Satz 1 bewiesen.

Satz 2. Zwei Kettenbrüche sind dann und nur dann gleich, wenn sie identisch sind. Dabei ist bei abbrechenden Kettenbrüchen der leicht wegzutransformierende Fall, daß der letzte Nenner 1 ist, auszuschließen.

I, 131 *Beweis.* Sei

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

ein Kettenbruch, dann ist, weil nach Voraussetzung und Satz 1

$$0 < \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}} < 1$$

ist, a_1 als größtes Ganze von $\frac{1}{\alpha}$ eindeutig bestimmt. Ferner ist dann, weil wieder nach Voraussetzung und Satz 1

$$0 < \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}} < 1$$

ist a_2 als größtes Ganze von $\frac{1}{\frac{1}{\alpha} - a_1}$ eindeutig bestimmt etz $\cdots$ Falls der letzte Partialnenner eines Kettenbruchs 1 sein sollte, ersetze man zu Herstellung der eindeutigen Normalform den vorletzten a_{n-1} durch $a_{n-1} + 1$.

Aus dem Beweis zu Satz 2 folgt sofort

I, 132 **Satz 3.** Jede reelle Zahl α des Intervalls $0 < \alpha \leqq 1$ läßt sich eindeutig in einen Kettenbruch

$$\alpha = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

mit positiven Nennern a_i entwickeln, die entweder eine unendliche, oder eine mit $a_n > 1$ abbrechende Folge ganzer Zahlen bilden. Nur für $\alpha = 1$ wird

$$\alpha = \frac{1}{1}\,.$$

Da sich *jedes* reelle α eindeutig in der Form

$$\alpha = a_0 + \alpha_0\,; \quad 0 < \alpha_0 \leqq 1$$

schreiben läßt, folgt so für jedes reelle α eine Kettenbruchentwicklung (eindeutig):

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}\ ,$$

wo $a_0 \geqq 0$ für $\alpha > 0$ und $a_0 < 0$ für $\alpha \leqq 0$ ganzzahlig ist, und die a_i die vorige Bedeutung haben.

Satz 4. Die Kettenbruchentwicklung einer reellen Zahl α bricht dann und nur dann ab, wenn α rational ist.

Beweis: 1.) Ist die Kettenbruchentwicklung endlich, so ist α rational.
2.) Sei α rational, also auch der „echte" Kettenbruch

$$\cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

NB. Auch aus Eukl. Alg. zu folgern!

rational, dann sind auch alle Brüche

$$\frac{u_1}{v_1} = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}\ ; \quad \frac{u_2}{v_2} = \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}$$

rational, weil z. B.

$$\frac{u_1}{v_1} = \cfrac{1}{a_1 + \cfrac{u_2}{v_2}}\ , \ldots$$

Die Brüche $\frac{u_i}{v_i}$ seien reduziert. Dann folgt

$$\frac{u_2}{v_2} = \frac{v_1 - a_1 u_1}{u_1}$$

also weil v_1 prim zu u_1:

$$v_2 = u_1\ , \quad \text{ebenso } v_3 = u_2\ , \ldots$$

Die Reihe

I, 133

$$\frac{u_1}{v_1}\ ,\ \frac{u_2}{v_2}\ , \ldots$$

ist also gliedweise gleich

$$\frac{u_1}{v_1}\ ,\ \frac{u_2}{u_1}\ ,\ \frac{u_3}{u_2}\ , \ldots$$

Wäre nur die Kettenbruch–Entwicklung unendlich, so wären alle Brüche $\frac{u_i}{v_i} < 1$ positiv, also

$$v_1 > u_1 > u_2 > \cdots$$

Man käme also auf eine monoton abnehmende Folge positiver ganzer Zahlen, was unmöglich.

Wir betrachten noch die Näherungsbrüche für einen Kettenbruch

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots}}$$

Die ersten sind

$$\frac{p_0}{q_0} = \frac{a_0}{1}\,;\ \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}\,;\ldots$$

Man beweist wie oben die Rekursionsformeln:

$$\left\{\begin{array}{l} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{array}\right. \tag{3}$$

für die als Anfangswerte

$$\begin{array}{ll} p_{-2} = 0\,; & p_{-1} = 1 \\ q_{-2} = 1\,; & q_{-1} = 0 \end{array}$$

I, 134 zu nehmen sind.

Daraus ergibt sich für die numerische Berechnung das Schema:

		a_0	a_1	......
0	1	a_0	$a_0 a_1 + 1$	......
1	0	1	a_1	......

Ferner gilt:

$$\begin{vmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{vmatrix} = (-1)^{n+1} \tag{4}$$

$$\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^{n+1}}{q_n q_{n+1}} \tag{5}$$

Die q_n sind von a_0 unabhängig, also monoton wachsend, die p_n für $a_0 \geqq 0$ ebenfalls. Wieder oszillieren die $\frac{p_n}{q_n}$ in immer engeren Schranken um den Wert von α herum.

Matrizenschreibweise:

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} =$$

I, 135

b.) Quadratische Irrationalitäten.

Es ist von besonderem Interesse die Kettenbruchentwicklungen reeller quadratischer Irrationalzahlen zu untersuchen. Hierfür besteht nämlich der wichtige

Satz 4. Die Kettenbruchentwicklung jeder reellen quadratischen Irrationalzahl ist periodisch und umgekehrt ist jeder periodische Kettenbruch eine reelle quadratische Irrationalzahl.

Beweis. 1.) Sei

$$\alpha = (b_0, b_1, \ldots, b_k;\ a_1, \ldots, a_n;\ a_1, \ldots, a_n;\ \ldots)$$

ein periodischer Kettenbruch, dessen Nenner die in den Klammern eingeschlossenen Zahlen sind. Dann folgt zunächst

$$\alpha = b_0 + \cfrac{1}{b_1 + \ddots + \cfrac{1}{b_k + \cfrac{1}{\omega}}}$$

wo $\omega = a_1 + \frac{1}{a_2 + \ddots}$ gesetzt ist. Nach dem Vorhergehenden ist

$$\alpha = \frac{\omega p_k + p_{k-1}}{\omega q_k + q_{k-1}}$$

wenn p_ν, q_ν die Zähler u. Nenner der Näherungsbrüche von α bis zum ν–ten bezeichnen. Es genügt also die Behauptung für ω zu beweisen. Nun gilt für ω: I, 136

$$\omega = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\omega}}}$$

Bezeichnet also $\mathsf{P}_n, \mathsf{Q}_n$ die Zähler u. Nenner der Näherungsbrüche für ω, so ist

$$\omega = \frac{\omega \mathsf{P}_n + \mathsf{P}_{n-1}}{\omega \mathsf{Q}_n + \mathsf{Q}_{n-1}} \ ,$$

also genügt ω der quadratischen Gleichung

$$\omega^2 \mathsf{Q}_n + \omega(\mathsf{Q}_{n-1} - \mathsf{P}_n) - \mathsf{P}_{n-1} = 0$$

mit der Diskriminante

$$(6) \qquad \left\{ \begin{array}{rcl} \mathsf{D} & = & (\mathsf{Q}_{n-1} - \mathsf{P}_n)^2 + 4\mathsf{Q}_n \mathsf{P}_{n-1} \\ & = & (\mathsf{Q}_{n-1} + \mathsf{P}_n)^2 - 4(\mathsf{P}_n \mathsf{Q}_{n-1} - \mathsf{Q}_n \mathsf{P}_{n-1}) \\ & = & (\mathsf{Q}_{n-1} + \mathsf{P}_n)^2 - 4(-1)^n \end{array} \right.$$

Man sieht hiernach wie sich die Diskriminante von ω, d. h. im wesentlichen auch die in α steckende quadratische Irrationalität aus den Summen der reinen Periode von α bestimmt.

2.) Um auch die Umkehrung zu beweisen, bemerken wir zunächst, daß zwei Zahlen α, β, die durch lineare Transformation

$$\beta = \frac{a\alpha + b}{c\alpha + d} \ ; \quad ad - bc = \varepsilon = \pm 1$$

I, 137 auseinander hervorgehen, und die wir „*äquivalent*“ nennen wollen, abgesehen von endlich vielen Nennern dieselben Kettenbruchnenner, also wenn sie periodische Kettenbrüche sind, dieselbe Periode haben.

Daß dies umgekehrt der Fall ist, d. h. daß 2 Zahlen α, β die von einer bestimmten Stelle dieselben Kettenbruchnenner haben (insbesondere also 2 rationale Zahlen) äquivalent sind, ist klar. Denn ist*)

$$\begin{array}{rcl} \alpha & = & (a_0, a_1, \dots a_n;\ c_1, c_2, \dots) \\ \beta & = & (b_0, b_1, \dots b_m;\ c_1, c_2, \dots)\,, \end{array}$$

so kann man setzen

$$\begin{array}{rcl} \alpha & = & \dfrac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}} \\ \beta & = & \dfrac{\omega r_m + r_{m-1}}{\omega s_m + s_{m-1}} \end{array}$$

*) für rat. α, β kann man offenbar stets erreichen, daß $c_1 = 1$, d. h. $\omega = 1$ ist

wo die $\frac{p_\nu}{q_\nu}$, $\frac{r_\mu}{s_\mu}$ die Näherungsbrüche von α, β und $\omega = (c_1, c_2, \dots)$ ist. Demnach sind α und β mit ω, also auch untereinander äquivalent, vermöge der Substitution:[1]

$$\alpha = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \begin{pmatrix} r_m & r_{m-1} \\ s_m & s_{m-1} \end{pmatrix}^{-1}$$

Wir zeigen jetzt aber das Übereinstimmen der Kettenbruchentwicklungen zweier äquivalenter Zahlen von einer gewissen Stelle an, d. h. den Satz:

. . . . . .

[1] Neben der rechten der beiden Matrizen ist andeutungsweise »(β)« zu lesen.

Kapitel 2

Tagebuch II: November 1923 – Januar 1924

Eintragungen

2.1 Kettenbruchtheorie (Fortsetzung aus I.)

Basic arithmetic of periodic continued fractions. Satz 8 proves that there are only finitely many reduced numbers with fixed discriminant, which is equivalent to the finiteness of the class number of binary quadratic forms with fixed discriminant. This connection is presented in Part c), with forms replaced by modules.

II, 140

Satz 5. Die Kettenbruchentwicklungen zweier reellen Zahlen stimmen dann und nur dann von einer Stelle an überein, wenn beide Zahlen äquivalent sind, d. h. durch eine linear gebrochene, ganzzahlige Transformation der Determinante ± 1 auseinander hervorgehen.

Beweis: Es ist nur noch zu zeigen, daß für 2 äquivalente reelle Irrationalzahlen α, β die Kettenbruchentwicklungen von einer gewissen Stelle an übereinstimmen.*)

Sei

$$\beta = \frac{a\alpha + b}{c\alpha + d}; \quad ad - bc = \varepsilon = \pm 1.$$

und

$$\alpha = (a_0, a_1, \dots)$$

die Kettenbruchentwicklung für α. (Diese symbolische Schreibweise bedeutet stets, daß a_0 dem Kettenbruch als erstes Ganze vorangeht).

Schreibt man dann

$$\alpha = (a_0, a_1, \dots, a_n, a_{n+1})$$

und bezeichnet mit $\dfrac{p_\nu}{q_\nu}$ die Näherungsbrüche, so gilt

$$\alpha = \frac{p_n\alpha_{n+1} + p_{n-1}}{q_n\alpha_{n+1} + q_{n-1}} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} (\alpha_{n+1})$$

also

$$\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} (\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} (\alpha_{n+1})$$

II, 141

Sei

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} r_n & r_{n-1} \\ s_n & s_{n-1} \end{pmatrix}$$

*) Nachweis einfacher durch *Erzeugung* der Modulgruppen

d. h.

$$\beta = \begin{pmatrix} r_n & r_{n-1} \\ s_n & s_{n-1} \end{pmatrix} (\alpha_{n+1}),$$

so ist

$$\begin{aligned} r_n &= ap_n + bq_n\,; & r_{n-1} &= ap_{n-1} + bq_{n-1} \\ s_n &= cp_n + dq_n\,; & s_{n-1} &= cp_{n-1} + dq_{n-1} \end{aligned}$$

und die Größen r_n, s_n genügen offenbar den Rekursionsformeln

$$\begin{aligned} r_{n+1} &= a_{n+1} r_n + r_{n-1} \\ s_{n+1} &= a_{n+1} s_n + s_{n-1}\,, \end{aligned}$$

sowie der Bedingung

$$\begin{vmatrix} r_n & r_{n-1} \\ s_n & s_{n-1} \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \cdot \begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = (-1)^{n+1}\varepsilon$$

Es ist speziell:

$$s_n = q_n \left(c\,\frac{p_n}{q_n} + d \right).$$

Da q_n positiv und $\frac{p_n}{q_n} \longrightarrow \alpha$, so kann man durch passende Normierung des willkürlichen Vorzeichens von a, b, c, d erreichen, daß für hinreichend hohes n das Vorzeichen von s_n mit dem von $c\alpha + d$ übereinstimmt, das wir positiv voraussetzen dürfen (α irrational!) Dann werden aber von einem gewissen n an die Größen s_n monoton wachsen. n sei so groß gewählt, daß schon

$$0 < s_{n-1} < s_n < s_{n+1} < \cdots$$

Dann entwickeln wir den rationalen Bruch $\frac{r_n}{s_n}$ in einen endlichen Kettenbruch: II, 142

$$\frac{r_n}{s_n} = (b_0, b_1, \ldots, b_m).$$

Es sei der vorletzte Näherungsbruch

$$(b_0, b_1, \ldots, b_{m-1}) = \frac{r'}{s'}\,,$$

so daß also

$$\begin{vmatrix} r' & r_n \\ s' & s_n \end{vmatrix} = (-1)^m$$

(nach (4), S. 134]), d. h.

$$r_n s' - s_n r' = (-1)^{m+1} \tag{7}$$

Man kann durch ev. Anfügen oder Weglassen eines letzten Nenners 1 in bekannter Weise erreichen, daß m nach Belieben gerade oder ungerade ist, und dies sei so gemacht, daß $(-1)^{m+1} = (-1)^{n+1}\varepsilon$ ist.

Ferner ist in der endlichen Kettenbruchentwicklung

$$s_n \geqq s' \geqq 0, \tag{8}$$

worin aber bei hinreichend hoher Wahl von n die Gleichheitszeichen vermieden werden können.

Durch die Bedingungen (7) u. (8) sind aber bekanntlich r', s' eindeutig für ein teilerfremdes Paar r_n, s_n bestimmt, also:

$$\begin{aligned} r_{n-1} &= r' \\ s_{n-1} &= s' \end{aligned}$$

und somit

$$(b_0, b_1, \ldots, b_m, \alpha_{n+1}) = \frac{\alpha_{n+1} r_n + r_{n-1}}{\alpha_{n+1} s_n + s_{n-1}} = \beta$$

$$\beta = (b_0, b_1, \ldots\ b_m;\ a_{n+1}, a_{n+2}, \ldots).$$

II, 143 w. z. b. w. Von dem hiermit bewiesenen Satz 5 haben wir nunmehr Anwendung auf die Fortführung des Beweises 2) von Satz 4 zu machen.

Um zu zeigen, daß die Kettenbruchentwicklung jeder reellen quadratischen Irrationalzahl periodisch ist, dürfen wir nach Satz 5 eine geeignet gewählte äquivalente Irrationalzahl dem Beweis zugrundelegen. Das führt auf den Begriff der *reduzierten* Zahlen, der im wesentlichen so konstruiert wird, daß rein–periodische Kettenbruchentwicklungen resultieren.

Definition. Eine reelle quadratische Irrationalzahl $\alpha = a + b \cdot \sqrt{d}$ heißt reduziert, wenn $\alpha > 1$ und $-1 < \alpha' < 0$ ist $(\alpha' = a - b\sqrt{d})$.

Dann gilt:

Satz 6. *Jede reelle quadratische Irrationalzahl des Körpers* $\mathsf{R}(\sqrt{d})$ *ist mit einer reduzierten Zahl aus* $\mathsf{R}(\sqrt{d})$ *äquivalent.*

Beweis: Sei

$$\omega = (a_0, a_1, \ldots\ a_{n-1}, \omega_n)$$

die abgebrochene Kettenbruchentwicklung einer Irrationalität ω aus $\mathsf{R}(\sqrt{d})$, und

$$\omega = \frac{p_{n-1}\omega_n + p_{n-2}}{q_{n-1}\omega_n + q_{n-2}}\,,$$

so gehört auch ω_n zu $\mathsf{R}(\sqrt{d})$. Durch Auflösung folgt

$$\omega_n = -\frac{q_{n-2}\omega - p_{n-2}}{q_{n-1}\omega - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} - \frac{(-1)^n}{q_n(q_{n-1}\omega - p_{n-1})}$$

Die Substitution $\sqrt{d} : -\sqrt{d}$ gibt: II, 144

$$\omega'_n = -\frac{q_{n-2}\omega' - p_{n-2}}{q_{n-1}\omega' - p_{n-1}} = -\frac{q_{n-2}}{q_{n-1}} \cdot \frac{\omega' - \frac{p_{n-2}}{q_{n-2}}}{\omega' - \frac{p_{n-1}}{q_{n-1}}}$$

$$\omega'_{n+1} = \frac{1}{q_{n-1}}\left(q_{n-1} - q_{n-2} - \frac{(-1)^n}{q_{n-1}\left(\omega' - \frac{p_{n-1}}{q_{n-1}}\right)}\right)$$

Für $n \longrightarrow \infty$ wird

$$\omega' - \frac{p_n}{q_n} \longrightarrow \omega' - \omega \neq 0$$

Nun ist für hinlänglich großes n sicher ω_n positiv und größer als 1, da dies ja schon für $n \geqq 1$ eintritt. Ferner wird nach den obigen Formeln wegen

$$\begin{aligned} \omega' - \frac{p_{n-1}}{q_{n-1}} &\quad\longrightarrow\quad \neq 0 \\ \omega' - \frac{p_{n-2}}{q_{n-2}} &\quad\longrightarrow\quad \neq 0 \end{aligned}$$

einmal ω'_n im Vorzeichen schließlich mit $-\frac{q_{n-2}}{q_{n-1}}$ also mit -1 übereinstimmen, und andererseits $\omega'_n + 1$ positiv sein, weil

$$q_{n-1}\left(\omega' - \frac{p_{n-1}}{q_{n-1}}\right) \longrightarrow \infty, \quad \text{da} \quad q_{n-1} \longrightarrow \infty$$

und $q_{n-1} - q_{n-2} \geqq 1$ ist. Also ist ω_n reduziert, und daher ω zu dem reduzierten ω_n äquivalent. II, 145

Entwickelt man nun eine reduzierte Zahl α in einen Kettenbruch, so führt der erste Schritt auf

$$\alpha = a_0 + \frac{1}{\alpha_1}\,,$$

wo $a_0 = [\alpha]$ ist, also

$$0 < a_0 < \alpha < a_0 + 1.$$

Dann muß aber auch α_1 reduziert sein. Denn es ist

$$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{1}{\alpha - [\alpha]} > 1\,,$$

und ferner

$$\alpha_1' = \frac{1}{\alpha' - a_0}$$

Es ist aber

$$-\infty < -1 - a_0 < \alpha' - a_0 < -a_0 \leqq -1$$

also

$$-1 < \alpha_1' = \frac{1}{\alpha' - a_0} < 0$$

d. h. α_1 reduziert.

Bei beliebiger Fortsetzung

$$\alpha = a_0 + \cfrac{1}{a_1 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{\alpha_n}}} = (a_0, a_1, \ldots\ a_{n-1}, \alpha_n)$$

werden also alle Schlußzahlen α_n reduziert sein. Gelingt es also nachzuweisen, daß die Anzahl der reduzierten Zahlen, die hier auftreten können, eine endliche ist, so wird die Periodizität der Kettenbruchentwicklungen reduzierter Zahlen und damit nach Satz 5 und 6 aller quadratischen Irrationalzahlen gezeigt sein, denn wenn eine Schlußzahl α_n zum zweitenmal auftritt, folgt die ganze Reihe der vom ersten α_n an erhaltenen Schlußzahlen periodisch weiter.

II, 146

Wir zeigen nun zuerst die Endlichkeit des in Frage kommenden Systems reduzierter Zahlen, dann noch etwas Eingehenderes über die auftretenden Perioden.

Da alle äquivalenten Zahlen zum selben Körper $\mathsf{R}(\sqrt{d})$ gehören, wäre die Endlichkeit der reduzierten Zahlen aus $\mathsf{R}(\sqrt{d})$ zu zeigen. Diese sind jedoch keineswegs nur in endlicher Anzahl vorhanden, vielmehr muß noch eine weitere Invarianz gegen die Äquivalenz beachtet werden:

Ist d quadratfrei, ganz, positiv und

$$\alpha = x + y\sqrt{d},$$

so genügt α der Gleichung: II, 147

$$\alpha^2 - 2x\alpha + x^2 - dy^2 = 0$$

die im allgemeinen nicht ganzzahlig ist. Wir setzen

$$x^2 - dy^2 = -\frac{a}{c}\,; \quad 2x = \frac{b}{c}$$

mit ganzen, teilerfreien a, b, c und erhalten als primitive (eindeutig durch α bestimmte) Gleichung:

$$c\alpha^2 - b\alpha - a = 0$$

mit der Diskriminante

$$D = b^2 + 4ac = 4c^2y^2d \ (\equiv 0, 1 \mod 4)$$

Dann ist D allen zu α äquivalenten Zahlen eigentümlich:

Satz 7. Äquivalente quadratische Irrationalzahlen haben gleiche Diskriminante (Gleichungsdiskriminante ihrer primitiven Gleichung).

Beweis: Sei

$$\beta = \frac{u\alpha + v}{w\alpha + s}\,; \quad \begin{vmatrix} u & v \\ w & s \end{vmatrix} = \pm 1.$$

Genügt β der Gleichung

$$c'\beta^2 - b'\beta - a' = 0,$$

so folgt durch bekannte Schlußweisen:

$$D' = b'^2 + 4a'c' = \begin{vmatrix} u & v \\ w & s \end{vmatrix}^2 (b^2 + 4ac) = D.$$

Wir haben demnach nur zu zeigen, daß folgender Satz richtig ist: **Satz 8.** *Es gibt nur endlich viele reduzierte Zahlen fester Diskriminante* D. II, 148

Beweis: Sei α eine reell–quadratische Irrationalität mit der Diskriminante D und der primitiven Gleichung

$$c\alpha^2 - b\alpha - a = 0\,; \quad b^2 + 4ac = \mathsf{D}.$$

Dann ist etwa

$$\alpha = \frac{b + \sqrt{\mathsf{D}}}{2c}\,; \qquad \alpha' = \frac{b - \sqrt{\mathsf{D}}}{2c}$$

$$\alpha = \frac{-2a}{b - \sqrt{\mathsf{D}}}\,; \qquad \alpha' = \frac{-2a}{b + \sqrt{\mathsf{D}}}$$

Ist nun α reduziert, so muß sein

$$0 < -\alpha' < 1 < \alpha\,,$$

also

$$0 < \frac{\sqrt{\mathsf{D}} - b}{2c} < 1 < \frac{\sqrt{\mathsf{D}} + b}{2c}\,.$$

Wir dürfen ohne Beschränkung $c > 0$ annehmen. Das Vorzeichen von $\sqrt{\mathsf{D}}$ muß dann positiv sein, da aus

$$\sqrt{\mathsf{D}} - b < \sqrt{\mathsf{D}} + b$$

folgt

$$b > 0,$$

und dann aus $\sqrt{\mathsf{D}} - b > 0$ auch $\sqrt{\mathsf{D}} > 0$. Es ist also dann

$$c > 0$$

$$0 < b < \sqrt{\mathsf{D}}.$$

Aus

$$0 < \frac{2a}{\sqrt{\mathsf{D}} + b} < 1 < \frac{2a}{\sqrt{\mathsf{D}} - b}$$

folgt dann noch

$$a > 0$$

II, 149 Aus $\mathsf{D} = b^2 + 4ac$ folgt

$$\mathsf{D} - b^2 = 4ac,$$

und da für b nur endlich viele Werte zur Verfügung stehen, stehen auch für a, c nur endlich viele zur Verfügung, w. z. b. w.

Damit ist Satz 4 nunmehr bewiesen. Wir erkennen überdies noch eine weitere Eigenschaft der reduzierten Zahlen:

Satz 8. *Jede reduzierte Zahl α hat eine reinperiodische Kettenbruch–Entwicklung.*

Beweis: Sei α reduziert und α_{n+1} die erste Schlußzahl in

$$\alpha = (a_1, a_2, \ldots, a_n;\, a_{n+1}),$$

die mit einer früheren übereinstimmt, so muß

$$\alpha_{n+1} = \alpha$$

sein. Denn in einer solchen Entwicklung ist jede Schlußzahl α_ν durch die nächstfolgende $\alpha_{\nu+1}$ *auch* eindeutig bestimmt (nicht nur umgekehrt). Ist nämlich

$$\alpha_\nu = a_\nu + \frac{1}{\alpha_{\nu+1}}\,,$$

so folgt

$$\begin{aligned}\alpha_{\nu+1} &= +\frac{1}{\alpha_\nu - a_\nu}\\ -\frac{1}{\alpha_{\nu+1}} &= a_\nu + \frac{1}{\frac{-1}{\alpha_\nu}}\end{aligned}$$

und folglich für die konjugierten: II, 150

$$-\frac{1}{\alpha'_{\nu+1}} = a_\nu + \frac{1}{-\frac{1}{\alpha'_\nu}}$$

Nun ist $-\frac{1}{\alpha'_{\nu+1}}$ reduziert, weil es $\alpha_{\nu+1}$ ist, also weil auch $-\frac{1}{\alpha'_\nu}$ reduziert ist, diese Gleichung der Anfang der Kettenbruchentwicklung*) von $-\frac{1}{\alpha'_{\nu+1}}$. Es ist daher α'_ν durch $\alpha'_{\nu+1}$ und somit α_ν durch $\alpha_{\nu+1}$ eindeutig bestimmt.

Wäre nun $\alpha_{n+1} = \alpha_\nu$ das erste Übereinstimmen, so folgte auch $\alpha_n = \alpha_{\nu-1}$, gegen die Voraussetzung. Also ist $\alpha_\nu = \alpha$.

Es gilt auch die Umkehrung von Satz 8

Satz 9. *Jeder rein–periodische Kettenbruch*

$$\alpha = (a_1, a_2, \ldots\, a_n;\, a_1, a_2, \ldots\, a_n;\, \ldots)$$

stellt eine reduzierte Zahl dar.

Beweis: 1.) Aus $a_1 \geqq 1$ folgt $\alpha > 1$.
2.) Wir haben α' zu bilden. Ich behaupte

$$-\frac{1}{\alpha'} = (a_n, a_{n-1}, \ldots\, a_1;\, a_n, a_{n-1}, \ldots\, a_1;\, \ldots).$$

Es besteht nämlich das Gleichungssystem II, 151

*) d. h. $a_\nu = \left[-\frac{1}{\alpha'_{\nu+1}}\right]$, wie man leicht aus der Reduziertheit von $-\frac{1}{\alpha'_\nu}$ u. $-\frac{1}{\alpha'_{\nu+1}}$ folgert.

$$\alpha = a_1 + \frac{1}{\alpha_1}\,; \quad \alpha_1 = a_2 + \frac{1}{\alpha_2}\,; \ \ldots\,; \quad \alpha_{n-1} = a_n + \frac{1}{\alpha}$$

und hieraus folgt wie oben

$$-\frac{1}{\alpha'_1} = a_1 + \frac{1}{-\frac{1}{\alpha'}}\,; \quad -\frac{1}{\alpha'_2} = a_2 + \frac{1}{-\frac{1}{\alpha'_1}}\,; \ \ldots\,; \quad -\frac{1}{\alpha'} = a_n + \frac{1}{-\frac{1}{\alpha'_{n-1}}}$$

wo jedesmal die a_ν die größten ganzen sind, weil die $-\frac{1}{\alpha'_\nu}$ sämtlich reduziert. Daraus folgt

$$-\frac{1}{\alpha'} = a_n + \cfrac{1}{a_{n-1} + \cdots + \cfrac{1}{a_1 + \cfrac{1}{-\cfrac{1}{\alpha'}}}} = (a_n, \ldots, a_1; \ldots)$$

Aus $a_n \geqq 1$ folgt dann sofort $-\frac{1}{\alpha'} > 1$, also

$$-1 < \alpha' < 0, \qquad \text{w. z. b. w.}$$

Gleichzeitig gilt:

Satz 10. *Die Kettenbruchperioden der Zahlen α, $-\frac{1}{\alpha'}$ gehen für reduziertes α durch Inversion auseinander hervor.*

Hieraus folgt noch ein spezielles Resultat über die Kettenbruchentwicklung einer $\sqrt{\mathsf{D}}$, wo D ganz und keine Quadratzahl ist.

Offenbar ist dann $\sqrt{\mathsf{D}}$ noch nicht reduziert. Beginnt man aber die Kettenbruchentwicklung

$$\sqrt{\mathsf{D}} = a_0 + \frac{1}{\alpha}\,,$$

II, 152 also $a_0 = \left[\sqrt{\mathsf{D}}\right]$, so ist $\alpha = \frac{1}{\sqrt{\mathsf{D}} - a_0}$ reduziert, weil

$$\alpha = \frac{1}{\sqrt{\mathsf{D}} - a_0} > 1$$

und $-1 < \alpha' = \frac{1}{-\sqrt{\mathsf{D}} - a_0} < 0$ ist.

Daher gilt

$$\sqrt{\mathsf{D}} = (a_0;\, a_1, a_2, \ldots\, a_n;\, a_1, \ldots\, a_n;\, \ldots)$$

Weiter ist nach Satz 10:

$$-\frac{1}{\alpha'} = \sqrt{\mathsf{D}} + a_0 = (a_n, a_{n-1}, \dots a_1;\ a_n, \dots a_1;\ \dots)$$

also:

$$\begin{aligned}&(2a_0;\ a_1, a_2, \dots, a_n;\ \dots)\\ =&(a_n;\ a_{n-1}, \dots a_1;\ a_n, \dots)\end{aligned}$$

d. h.

$$\begin{array}{ccc} 2a_0 & = & a_n \\ a_1 & = & a_{n-1} \\ \multicolumn{3}{c}{\dots\dots\dots\dots\dots} \\ a_\nu & = & a_{n-\nu} \\ \multicolumn{3}{c}{\dots\dots\dots\dots\dots} \end{array}$$

Die Kettenbruchentwicklung von $\sqrt{\mathsf{D}}$ sieht also stets so aus

$$\sqrt{\mathsf{D}} = (a_0;\ a_1, a_2, \dots, a_2, a_1, 2a_0;\ \dots)$$

Satz 11. *Ist* D *eine ganze Nichtquadratzahl, so besteht die Kettenbruchentwicklung der positiven* $\sqrt{\mathsf{D}}$ *aus einer eingliedrigen Vorperiode* a_0*, einer symmetrischen Folge* $(a_1, \dots a_{n-1}) = (a_{n-1}, \dots, a_1)$ *und dem Periodenschlußglied* $a_n = 2a_0$. II, 153

c.) Beziehung zur Modultheorie.

Sei $\mathsf{R}(\sqrt{d})$ ein reeller quadratischer Zahlkörper mit der Diskriminante d. Wir betrachten dann „Moduln“ im Bereich der ganzen Zahlen von $\mathsf{R}(\sqrt{d})$, d. h. Systeme ganzer Zahlen, die sich durch Addition und Subtraktion reproduzieren. Die Anzahl der linear unabhängigen Zahlen eines Moduls aus $\mathsf{R}(\sqrt{d})$ kann nur 1 oder 2 sein. Wir betrachten allein „2 gliedrige Moduln“. Nach allgemeinen Prinzipien haben diese eine Basisdarstellung

$$\alpha = c_1\omega_1 + c_2\omega_2$$

durch 2 Basiselemente ω_1, ω_2. Jeder Modul lässt sich, wenn $1, \omega$ eine Körperbasis ist, im Gitter $x + \omega y$ als ein übergelagertes Parallelgitter deuten, das den Nullpunkt enthält, und jedes solche Parallelgitter liefert einen Modul.

Die Basis ω_1, ω_2 eines Moduls läßt sich auf folgende Weise eindeutig normieren. Wie man sofort sieht enthält jeder Modul unendlich viele ganze rationale

Zahlen. Sei a die kleinste, dann sind alle übrigen Multipla von a. Sei ferner unter allen Zahlen $x+\omega y$ des Moduls $b'+c\omega$ eine solche, deren $y=c$ positiv,
II, 154 möglichst klein ist, dann sind alle auftretenden y Multipla von c. Ferner kommt im Modul auch $b+c\omega$ vor, wo b der kleinste positive Rest von $b' \mod a$ ist. Es ist dann

$$(a, b+c\omega)$$

eine Basis des Moduls, und zwar offenbar eindeutig normiert.

Satz 12. *Ein 2 gliedriger Modul im reell–quadratischen Zahlkörper* $\mathsf{R}(\sqrt{d})$ *mit der Basis* $1, \omega$ *ist durch Angabe dreier Zahlen* a, b, c *charakterisiert, die die normierte Basis*

$$(a, b+c\omega)$$

bilden. a, b, c *sind als Invarianten des Moduls anzusehen.*

Natürlich können a, b, c ganz willkürlich gewählt werden, nur den Bedingungen:

$$a>0\,; \quad c>0$$
$$a>b\geqq 0$$

genügend. Falls der Modul ein „Ideal“ sein soll, müssen jetzt a, b, c noch weiteren Bedingungen genügen ($c \mid a$, etz).

Umgekehrt können im übrigen zwei Moduln (a, b, c) und (a', b', c') jedenfalls
II, 155 nur dann gleich sein, wenn $a=a'$, $c=c'$ ist, da a, c invariant definiert sind. Aus der Relation zwischen zwei verschiedenen Basen desselben Moduls:

$$(\omega_1', \omega_2') = \begin{pmatrix} p & q \\ r & s \end{pmatrix} (\omega_1, \omega_2)\,; \qquad \begin{vmatrix} p & q \\ r & s \end{vmatrix} = \pm 1$$

folgert man dann leicht, daß auch $b=b'$ sein muß

Satz 13. *Durch die Invarianten* a, b, c *ist ein Modul eindeutig bestimmt.*

Zwei Moduln heißen *äquivalent*, wenn sie durch Multiplikation ihrer sämtlichen Zahlen mit (einer u. derselben) ganzen oder gebrochenen Körperzahl ineinanderübergeführt werden können.

Hiernach zerfallen alle Moduln in *Klassen* nicht äquivalenter, und es ist leicht zu sagen, daß es unendlich viele solcher Klassen gibt.

Jedem Modul ist nämlich als Invariante zugeordnet ein bestimmtes Ideal, nämlich der größte gemeinsame Teiler aller Modulzahlen, d. h. schon der beiden Basiszahlen. In Dedekindschem Sinne ist der Modul teilbar durch dieses Ideal, weil alle Zahlen des Moduls zum Ideal gehören. Ist der Modul selbst Ideal, so ist

er mit dem ihm so zugeordneten Ideal und seine Klasse mit der entsprechenden Idealklasse identisch. Außer diesen endlich vielen Idealklassen gibt es aber noch weitere unendlich viele Modulklassen. II, 156

Bildet man nämlich das Determinantenquadrat

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2$$

einer Modulbasis, so ist dasselbe eine ganze rationale Zahl, deren (positiver) Wert, wie aus der speziellen Basis $(a, b + c\omega)$ ersichtlich, gleich $da^2c^2 = d \times$ (Anzahl d. Restkl.)^2 ist. Da die Anzahl d. Restklassen nach dem zugeordneten Ideal $\mathfrak{a}$ gleich $(N\mathfrak{a})^2$ ein Teiler der Anzahl der Restklassen nach dem Modul sein muß, weil das Ideal $\mathfrak{a}$ den Modul teilt, ist der Quotient

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 \cdot \frac{1}{(N\mathfrak{a}^2)d}$$

eine ganze rationale (wegen $d > 0$ positive) Zahl und Invariante des Moduls, aber auch der zugeordneten *Modulklasse*.

Sind nämlich $\mathfrak{M}_1, \mathfrak{M}_2$ zwei Moduln und

$$\mathfrak{M}_1\lambda_1 = \mathfrak{M}_2\lambda_2$$

ferner $\mathfrak{a}_1, \mathfrak{a}_2$ die zugehörigen Ideale, so ist

$$\mathfrak{a}_1\lambda_1 = \mathfrak{a}_2\lambda_2$$

II, 157

Die Quotienten für $\mathfrak{M}_1\lambda_1, \mathfrak{M}_2\lambda_2$ sind gleich:

$$\begin{vmatrix} \lambda_1\omega_1, & \lambda_1\omega_2 \\ \lambda_1'\omega_1', & \lambda_1'\omega_2' \end{vmatrix}^2 \frac{1}{N(\mathfrak{a}_1\lambda_1)^2 d} = \begin{vmatrix} \lambda_2\theta_1, & \lambda_2\theta_2 \\ \lambda_2'\theta_1', & \lambda_2'\theta_2' \end{vmatrix}^2 \frac{1}{N(\mathfrak{a}_2\lambda_2)^2 d}$$

Durch Wegheben des Faktors $\lambda_1^2{\lambda_1'}^2 = N(\lambda_1^2)$ und $(\lambda_2^2{\lambda_2'}^2) = N(\lambda_2^2)$ entsteht:

$$\begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 \frac{1}{(N\mathfrak{a}_1^2)d} = \begin{vmatrix} \theta_1 & \theta_2 \\ \theta_1' & \theta_2' \end{vmatrix}^2 \frac{1}{(N\mathfrak{a}_2^2)d}$$

w. z. b. w.

Dieser jedem Modul $\mathfrak{M}$ eindeutig zugeordnete, ganze rationale, positive Quotient $\boldsymbol{\partial} = \begin{vmatrix} \omega_1 & \omega_2 \\ \omega_1' & \omega_2' \end{vmatrix}^2 \frac{1}{N\mathfrak{a}^2 d}$ heißt die Diskriminante von $\mathfrak{M}$.

Satz 14. *Die Diskriminante $\boldsymbol{\partial}$ von $\mathfrak{M}$ ist eine Invariante der Modulklasse von $\mathfrak{M}$.*

Nun ist speziell für $\mathfrak{a} = 1$, also Moduln der Form $(1, c\omega)$:

$$\boldsymbol{\partial} = \begin{vmatrix} 1 & c\omega \\ 1 & c\omega' \end{vmatrix}^2 : \begin{vmatrix} 1 & \omega \\ 1 & \omega' \end{vmatrix}^2 = c^2$$

Da c beliebig ist, gibt es unendlich viele Modulklassen.

II, 158 **Satz 15.** *Es gibt unendlich viele Modulklassen.*

Den Modulklassen lassen sich nun die möglichen Kettenbruchperioden aus $\mathsf{R}(\sqrt{d})$ gegenseitig eindeutig zuordnen.

Jedem Modul (ω_1, ω_2) ordnen wir zunächst den Basisquotienten $\frac{\omega_1}{\omega_2} = \alpha$ zu. Basistransformationen entsprechen linear gebrochen mit der Determinante ± 1 zusammenhängende α, also gleiche Kettenbruchperioden der Basisquotienten α. Jedem Modul ist so eine Kettenbruchperiode eindeutig zugeordnet. Diese ist sogar der ganzen Modulklasse eigentümlich. Denn ist $(\vartheta_1, \vartheta_2)$ ein äquivalenter Modul und mit ganzen λ_1, λ_2:

$$\lambda_1(\omega_1, \omega_2) = \lambda_2(\vartheta_1, \vartheta_2)$$

wofür auch unbedenklich

$$(\omega_1, \omega_2) = \frac{\lambda_2}{\lambda_1}(\vartheta_1, \vartheta_2) = \lambda(\vartheta_1, \vartheta_2)$$

mit gebrochenem λ geschrieben werden kann, so sind $\frac{\lambda_1\omega_1}{\lambda_1\omega_2} = \frac{\omega_1}{\omega_2}$ und $\frac{\lambda_2\vartheta_1}{\lambda_2\vartheta_2} = \frac{\vartheta_1}{\vartheta_2}$

II, 159 zwei äquivalente Basisquotienten, haben also gleiche Kettenbruchperiode. Sind umgekehrt α, β zwei Zahlen gleicher Kettenbruchperiode, die als Basisquotienten zweier Moduln $\mathfrak{M}, \mathfrak{N}$ auftreten:

$$\alpha = \frac{\omega_1}{\omega_2}; \quad \beta = \frac{\vartheta_1}{\vartheta_2}$$

so folgt aus

$$\beta = \frac{p\alpha + q}{r\alpha + s}; \quad \begin{vmatrix} p & q \\ r & s \end{vmatrix} = \pm 1$$

$$\begin{aligned} \vartheta_1 &= \lambda(p\omega_1 + q\omega_2) &= \lambda\overline{\omega}_1 \\ \vartheta_2 &= \lambda(r\omega_1 + s\omega_2) &= \lambda\overline{\omega}_2 \end{aligned}$$

wo λ eine gebrochene Zahl aus $\mathsf{R}(\sqrt{d})$ ist, und $\overline{\omega}_1, \overline{\omega}_2$ ebenfalls Basis für $\mathfrak{M}$ ist. $\mathfrak{M}$ und $\mathfrak{N}$ sind daher in der Beziehung

$$\lambda\mathfrak{M} = \mathfrak{N},$$

d. h. äquivalent.

Satz 16. *Den verschiedenen Modulklassen entsprechen gegenseitig eindeutig die verschiedenen Kettenbruchperioden von* $\mathsf{R}(\sqrt{d})$ (*als Kettenbruchperioden der Basisquotienten*). II, 160

d.) Die Pellsche Gleichung, Einheiten.

Es sei ω eine reell–quadratische Irrationalzahl, die wir reduziert voraussetzen, und

$$c\omega^2 - b\omega - a = 0$$

die zugehörige Gleichung mit der Diskriminante $\mathsf{D} = b^2 + 4ac$, wobei a, b, c ihre gemeinsamen Teiler sind. Die Kettenbruchentwicklung von ω ist rein periodisch:

$$\omega = (a_1, a_2, \dots a_n; \dots)$$

also

$$\omega = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}}$$

Das liefert

$$q_n\omega^2 - (p_n - q_{n-1})\omega - p_{n-1} = 0$$

also mit ganzzahligem u:

$$\begin{aligned} q_n &= uc \\ p_n - q_{n-1} &= ub \\ p_{n-1} &= ua \end{aligned}$$

Wir setzen noch

$$p_n + q_{n-1} = t.$$

Dann wird

$$p_n = \frac{t + ub}{2} \quad ; \quad p_{n-1} = ua$$

$$q_n = uc \quad ; \quad q_{n-1} = \frac{t - ub}{2}$$

II, 161 Da nun

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = (-1)^n$$

ist, folgt

$$\frac{t^2 - u^2 b^2}{4} - u^2 ac = (-1)^n$$

also

$$t^2 - u^2 \mathsf{D} = (-1)^n 4$$

Man erhält also auf folgende Weise eine Lösung der Pellschen Gleichung:

II, 162 **Satz 17.** *Ist ω eine reduzierte, reell quadratische Irrationalität mit der Diskriminante D, sind ferner $\frac{p_{n-1}}{q_{n-1}}$ und $\frac{p_n}{q_n}$ vorletzter und letzter Näherungsbruch vor Wiederkehr der (n gliedrigen) Periode der Kettenbruchentwicklung für ω, so liefert*

$$\begin{aligned} t &= p_n + q_{n-1} \\ u &= (q_n, p_n - q_{n-1}, p_{n-1}) \end{aligned}$$

eine Lösung der Pellschen Gleichung

$$t^2 - \mathsf{D}u^2 = (-1)^n 4$$

Man kann auch einfach

$$u = \frac{q_n}{c}\,; \quad t = p_n + q_{n-1}$$

setzen, wenn man die Gleichung für ω besitzt. Natürlich genügt es, u, t positiv zu wählen.

Beispiel.

$$\omega = \frac{1}{\sqrt{40} - 6} \quad \text{ist reduziert.}$$

Gleichung: $4\omega^2 - 12\omega - 1 = 0\,; \quad \mathsf{D} = 160$

Kettenbruchentwicklung:

$$\begin{array}{llll}
\omega = \frac{1}{\sqrt{40}-6} & = \frac{\sqrt{40}+6}{4} & = \frac{\sqrt{10}+3}{2} = 3 + \frac{1}{\omega_1} & \\
\omega_1 = \frac{1}{\frac{\sqrt{10}-3}{2}} & = \frac{2\sqrt{10}+6}{1} & = 12 + \frac{1}{\omega_2} & a_1 = 3 \\
\omega_2 = \frac{1}{2\sqrt{10}-6} & = \frac{\sqrt{10}+3}{2} & = \omega & a_2 = 12
\end{array}$$

$$\omega = (3, 12;\ 3, 12;\ \dots)$$

		3	12
0	1	3	37
1	0	1	12

$$n = 2 \qquad p_2 = 37 \qquad p_1 = 3$$
$$q_2 = 12 \qquad q_1 = 1$$

$$\left.\begin{aligned} (q_2, p_2 - q_1, p_1) = (12, 36, 3) = 3 \\ \frac{q_2}{c} = \frac{12}{4} = 3 \end{aligned}\right\} u = 3$$

$$t = p_2 + q_1 = 38$$
$$38^2 - 160 \cdot 3^2 = 4$$

Natürlich gilt Satz 17 auch, wenn n nicht die primitive Periode, sondern ein Vielfaches derselben ist. II, 163

Wir beweisen nun die Umkehrung von Satz 17.

Satz 18. *Ist ω eine reduzierte Zahl der Diskriminante D, so liefert das Verfahren von Satz 17 bei geeigneter Verfügung über n jede Lösung von*

$$t^2 - \mathsf{D}u^2 = \pm 4$$

in der $t, u > 0$ ist.

Beweis: Sei $t^2 - \mathsf{D}u^2 = \pm 4$ in positiven ganzen t, u und

$$c\omega^2 - b\omega - a = 0\,; \quad b^2 + 4ac = \mathsf{D}.$$

Wir setzen

$$p_n = \frac{t + ub}{2} \qquad p_{n-1} = ua$$
$$q_n = uc \qquad q_{n-1} = \frac{t - ub}{2}$$

Wegen

$$t^2 - \mathsf{D}u^2 \equiv t^2 - b^2u^2 \equiv (t+ub)(t-ub) \equiv 0 \mod 4$$

ist

$$t \pm ub \equiv 0 \mod 2,$$

also $p_n, q_{n-1}, p_{n-1}, q_n$ sämtlich ganzzahlig. Daraus folgt ferner

$$q_n\omega^2 - (p_n - q_{n-1})\omega - p_{n-1} = 0$$

also

$$\omega = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}}$$

und

$$\begin{vmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{vmatrix} = \frac{t^2 - u^2(b^2+4ac)}{4} = \pm 1$$

II, 164 je nach dem Vorzeichen in $t^2 - \mathsf{D}u^2 = \pm 4$. Ferner folgt

$$q_n - q_{n-1} = \frac{(2c+b)u - t}{2}\,.$$

Nun ist ω reduziert, also nach S. 148]

$$\sqrt{\mathsf{D}} - b < 2c,$$

d. h.

$$q_n - q_{n-1} > \frac{u\sqrt{\mathsf{D}} - t}{2} = \frac{\mathsf{D}u^2 - t^2}{2(u\sqrt{\mathsf{D}} + t)} = \frac{\mp 2}{u\sqrt{\mathsf{D}} + t}$$

Es ist aber wegen $t, u \geqq 1$ und $\mathsf{D} > 1$ sicher

$$u\sqrt{\mathsf{D}} + t > 2,$$

also, wenn $t^2 - \mathsf{D}u^2 = +4$:

$$q_n - q_{n-1} > -1,$$

wenn $t^2 - \mathsf{D}u^2 = -4$

$$q_n - q_{n-1} > 0.$$

Weil $q_n - q_{n-1}$ ganz ist, gilt also jedenfalls

$$q_{n-1} \leqq q_n,$$

wo das Gleichheitszeichen nur für „+4“ stehen kann.

Weiter ist wegen $b < \sqrt{\mathsf{D}}$ (S. 148])

$$\begin{aligned} q_{n-1} &= \frac{t - ub}{2} > \frac{t - u\sqrt{\mathsf{D}}}{2} = \frac{t^2 - \mathsf{D}u^2}{2(t + u\sqrt{\mathsf{D}})} \\ &= \frac{\pm 2}{t + u\sqrt{\mathsf{D}}}\,, \end{aligned}$$

also $q_{n-1} \geqq 0$, wo das Gleichheitszeichen nur für „−4“ stehen kann.

Insgesamt ist also

$$0 \leqq q_{n-1} \leqq q_n$$

mit den genannten Einschränkungen für d. Gleichh. zeichen. II, 165

Wir entwickeln nun $\frac{p_n}{q_n}$ in einen endlichen Kettenbruch, indem wir dabei die Anzahl n der Teilnenner so annehmen, daß $(-1)^n = \pm 1$ wird:

$$\frac{p_n}{q_n} = (a_1, a_2, \ldots, a_n)$$

Ist dann $\frac{p'}{q'}$ der vorletzte Näherungsbruch (der letzte ist wegen der Teilerfremdheit $\frac{p_n}{q_n}$ selbst). Dann ist

$$\begin{vmatrix} p_n & p' \\ q_n & q' \end{vmatrix} = (-1)^n = \pm 1,$$

also

$$p_n q' - q_n p' = \pm 1$$

und dabei

$$0 \leqq q' \leqq q_n\,,$$

wo das Gleichheitszeichen in der unteren Grenze nur für $n = 1$, also im Falle „-4“, in der oberen Grenze nur für $n = 2$, also im Falle „$+4$“ vorkommt. Da mit diesen Bedingungen $p_n x - q_n y = \pm 1$ eindeutig lösbar ist, folgt

$$q' = q_{n-1}$$
$$p' = p_{n-1}$$

also

$$\omega = (a_1, a_2, \dots a_n, \omega),$$

d. h. unsere Lösung entsteht aus einer Kettenbruchperiode von ω nach dem Schema von Satz 17, w. z. b. w.

II, 166

Hieraus folgt noch einiges Wichtige. t und u wachsen offenbar gleichzeitig, sodaß von einer kleinsten Lösung geredet werden kann, die mit T, U bezeichnet werden soll. Da u mit q_n und q_n mit n monoton wächst, resultiert T, U für möglichst kleines n, also bei der primitiven Periode. Daraus folgt, daß es zwei Sorten von D gibt, solche mit ungeradem n, für die $t^2 - \mathsf{D}u^2 = \pm 4$ beides lösbar ist und solche mit geradem n, für die $t^2 - \mathsf{D}u^2 = -4$ sicher nicht lösbar ist.

Satz 19. *Es gibt* 2 *Arten von Diskriminanten* D*, solche für die* $t^2 - \mathsf{D}u^2 = -4$ *unlösbar, und solche für die* $t^2 - \mathsf{D}u^2 = -4$ *lösbar ist. Sie unterscheiden sich dadurch, daß die Kettenbruchperioden der Zahlen der ersten Art von* D *sämtlich gerade Gliederzahl, die der zweiten Art sämtlich ungerade Gliederzahl haben.*

Die Lösungen von $t^2 - \mathsf{D}u^2 = \pm 4$ entsprechen Einheiten von $\mathsf{R}(\sqrt{\mathsf{D}})$. Es ist nämlich dann

$$\pm \frac{t \pm u\sqrt{\mathsf{D}}}{2}$$

ein System von 4 Einheiten $\pm\varepsilon, \pm\varepsilon^{-1}$. Eine und nur eine von ihnen ist > 1, nämlich

$$\varepsilon = \frac{t + u\sqrt{\mathsf{D}}}{2}\,.$$

II, 167

In bekannter Weise schließt man:

Satz 20. *Die sämtlichen Lösungen von* $\frac{t^2-\mathsf{D}u^2}{4} = \pm 1$ *entstehen aus der „Grundeinheit", d. h. der kleinsten Lösung* $\frac{T^2-\mathsf{D}U^2}{4} = \pm 1$*, indem man die Grundeinheit*

$$\varepsilon = \frac{T + U\sqrt{\mathsf{D}}}{2}$$

potenziert:

$$\varepsilon, \varepsilon^2, \ldots\ldots$$

und zu jeder Potenz ε^ν *die 4 Einheiten*

$$\pm\varepsilon^\nu, \pm\varepsilon^{-\nu}$$

nimmt. Den positiven Lösungen entsprechen die positiven Potenzen $\varepsilon, \varepsilon^2, \ldots$ *allein. Ausgeschlossen ist dabei die triviale Lösung*

$$\pm\frac{(\pm 2)^2 - \mathsf{D}\cdot 0^2}{4} = \pm 1,$$

die den Einheiten ± 1 *zugeordnet ist. Die Norm der Grundeinheit ist* ± 1*, je nachdem die Perioden von* D *gerade oder ungerade Gliederzahl haben.*

Nimmt man im Falle eines quadratischen Körpers $\mathsf{R}(\sqrt{d})$ der Diskriminante $d \equiv 0 \mod 4$ für ω eine zu $\frac{\sqrt{d}}{2}$ gehörige reduzierte Zahl, so ist das zugehörige $\mathsf{D} = 4\,\frac{d}{4} = d$ und man erhält eine Lösung von

$$t^2 - du^2 = \pm 4,$$

in der t notwendig gerade sein muß. Daher kann 4 wegdividiert werden und man erhält:

$$\left(\frac{t}{2}\right)^2 - \frac{d}{4}u^2 = \pm 1$$

$\frac{d}{4}$ ist dann quadratfrei, und die kleinste Lösung liefert die Grundeinheit von $\mathsf{R}(\sqrt{d})$: $\varepsilon = \frac{T}{2} + U\,\frac{\sqrt{d}}{2}$ II, 168

Ist aber $d \equiv 1 \mod 4$, so nehme man eine zu $\frac{1+\sqrt{d}}{2}$ gehörige reduzierte Zahl ω, deren Diskriminante $\mathsf{D} = d$ ist. Man erhält dann Lösungen von

$$\frac{t^2 - du^2}{4} = \pm 1$$

in denen wegen $d \equiv 1 \mod 4$ sicher

$$t^2 - u^2 \equiv 0 \mod 4$$

also t und u gerade oder ungerade sind.

$$\varepsilon = \frac{T + U\sqrt{d}}{2} = \frac{T-U}{2} + U\,\frac{1+\sqrt{d}}{2}$$

ist dann die Grundeinheit (ganzzahlig!), wenn T, U wieder die kleinste positive Lösung ist.

Allgemein liefern die reduzierten Zahlen eines D höhere Einheiten von $\mathsf{R}(\sqrt{d})$. D ist von d stets um ein Quadrat unterschieden. Der Zusammenhang ist folgender:

Ist ω irgendeine reell–quadratische Irrationalität der Diskriminante D, so gehört zu D eindeutig eine Körperdiskriminante d, sodaß

$$\mathsf{D} = m^2 d$$

ist, also $\mathsf{R}(\sqrt{\mathsf{D}}) = \mathsf{R}(\sqrt{d})$. Befreit man nämlich zuerst D von allen quadratischen Faktoren:

$$\mathsf{D} = q^2 \mathsf{D}_0\,; \quad \mathsf{D}_0 \text{ quadratfrei,}$$

II, 169

so ist entweder $\mathsf{D}_0 \equiv 1 \mod 4$, dann ist $d = \mathsf{D}_0$ zu setzen, oder aber $\mathsf{D}_0 \equiv 2, 3 \mod 4$. Da aber D als Zahldiskriminante ($b^2 + 4ac = \mathsf{D}$) stets $\equiv 0, 1 \mod 4$ ist, und $q^2 \equiv 0, 1 \mod 4$, so kann dieser Fall offensichtlich nur für $\mathsf{D} \equiv 0 \mod 4$, $q^2 \equiv 0 \mod 4$ eintreten. Dann ist $4\mathsf{D}_0 = d$ die zugehörige Körperdiskriminante und für $m = \frac{q}{2}$:

$$\mathsf{D} = m^2 d.$$

Satz 21. *Ist ω eine reell–quadratische Irrationalität aus $\mathsf{R}(\sqrt{d})$, so ist ihre Diskriminante D teilbar durch die Körperdiskriminante d und*

$$\mathsf{D} = m^2 d.$$

mit ganzem m.

II, 170

e.) Zahlringe in $\mathsf{R}(\sqrt{d})$.

Sei $\mathsf{R}(\sqrt{d})$ ein reell–quadratischer Körper der Diskriminante d. Wir betrachten dann den Zahlring R_m :

$$\boldsymbol{\alpha \equiv} \textbf{ rationaler, zu } \boldsymbol{m} \textbf{ primer Zahl mod } \boldsymbol{m}$$

für irgendeinen ganzen rationalen Modul m.

Satz 22. *Ist* $(1, \omega)$ *eine Basis von* $\mathsf{R}(\sqrt{d})$, *so sind alle und nur die Zahlen von* R_m *in der Form*

$$\alpha = a + bm\omega\,; \quad (a, m) = 1$$

mit ganzen a, b *enthalten, d. h.* $(1, m\omega)$ *ist eine Basis von* R_m .

Beweis: 1.) Ist $\alpha = a + bm\omega$, so ist

$$\alpha \equiv a \mod m\,; \quad (a, m) = 1$$

also α zu R_m .

2.) Ist $\alpha \equiv r \mod m\,; \quad (r, m) = 1$, so ist

$$\begin{aligned} \alpha &= r + \beta m = r + (c_1 + c_2\omega)m \\ &= r + c_1 m + c_2\omega m = a + b\omega m \end{aligned}$$

und $a = r + c_1 m$ prim zu m.

Satz 23. *Der Führer von* R_m *ist* m.

Beweis: Ist m' irgendein echter Teiler von m, so läßt sich die Zugehörigkeit zu R_m nicht mod m' charakterisieren. Wäre nämlich irgendeine ganze prime Restklasse mod m' in R_m enthalten, und a ein rationaler Repräsentant dieser Restklasse mod m, der prim zu m' gewählt werden darf, so ist

II, 171

$$a + m'\omega$$

sicherlich nicht in R_m enthalten, denn sonst wäre

$$\begin{array}{rcll} a + m'\omega & \equiv & r & \mod m \\ a + m'\omega' & \equiv & r & \mod m \\ \hline m'(\omega - \omega') & \equiv & 0 & \mod m \\ \omega - \omega' & \equiv & 0 & \mod \dfrac{m}{m'}\,, \end{array}$$

während $\omega - \omega' = \sqrt{d}$ sicher nicht durch eine rationale Zahl > 1 teilbar ist. Es ist also $a + m'\omega$ nicht in R_m enthalten, und daher R_m nicht mod m' definierbar, w. z. b. w.

Aus Satz 22 folgt noch:

Satz 24. *Der Ring R_m ist identisch mit dem Modul $(1, m\omega)$, wenn von den zu m nicht primen Modulzahlen abgesehen wird.*

Ist D die Diskriminante einer quadratischen Irrationalität α, so liefert die Kettenbruchentwicklung einer zu α reduzierten Zahl eine Einheit von R_m, wenn

$$\mathsf{D} = m^2 d.$$

Denn es wird eine Lösung von

$$t^2 - m^2 du^2 = \pm 4,$$

also

$$\varepsilon = \frac{t + mu\sqrt{d}}{2} \quad \text{geliefert, die}$$

II, 172 wegen $\omega = \frac{d+\sqrt{d}}{2}$ zu R_m gehört. Die kleinste Lösung von $t^2 - \mathsf{D}u^2 = \pm 4$ liefert dann offenbar die kleinste positive Einheit > 1 von R_m, d. h. die Grundeinheit von R_m.

Satz 25. *Ist $\mathsf{D} = m^2 d$ eine Zahldiskriminante aus $\mathsf{R}(\sqrt{d})$, so liefert die Kettenbruchentwicklung zu D gehöriger reduzierter Zahlen nach dem Schema von Satz 17 die sämtlichen Einheiten von R_m, speziell bei Abbruch nach der primitiven Periode die Grundeinheit von R_m.*

Wir sahen früher, daß die Diskriminanten D der Basisquotienten $\frac{\omega_1}{\omega_2}$ einer Modulklasse alle dieselben sind, ferner daß auch die Moduldiskriminante $\boldsymbol{\partial}$ Invariante der ganzen Modulklasse ist. Es liegt daher nahe eine Relation zwischen $\mathsf{D} = m^2 d$ (auch m ist invariant!) und $\boldsymbol{\partial}$ zu vermuten.

Man kann nachweisen, daß $\boldsymbol{\partial} = m^2$ ist.

II, 173 Dies ist zunächst klar, wenn der Modul den Idealteiler 1 hat. Denn ist dann:

$$\mathfrak{M} = (a, b + c\omega)$$

so ist

$$\boldsymbol{\partial} = a^2 c^2.$$

Andererseits ist der Basisquotient

$$\alpha = \frac{b + c\omega}{a}$$

der Quotient zweier relativ primer Zahlen. α genügt der Gleichung

$$a^2x^2 - aS(b + c\omega)x + N(b + c\omega) = 0$$

und diese ist primitiv, weil $N(b + c\omega)$ prim zu a ist. Daher wird ihre Diskriminante für $\omega = \frac{\sqrt{d}}{2}$

$$\begin{aligned} \mathsf{D} &= a^2\big(S(b + c\omega)\big)^2 - 4a^2N(b + c\omega) \\ &= 4a^2b^2 - 4a^2\left(b^2 - c^2\left(\frac{\sqrt{d}}{2}\right)^2\right) \\ &= a^2c^2d \end{aligned}$$

und für $\omega = \frac{1+\sqrt{d}}{2}$

$$\begin{aligned} \mathsf{D} &= 4a^2b^2 + 4a^2bc + a^2c^2 - 4a^2\left(b^2 + bc - c^2\frac{d-1}{4}\right) \\ &= a^2c^2d \end{aligned}$$

Ist dagegen der Idealteiler $(a, b + c\omega) = \mathfrak{a}$, so ist

$$\boldsymbol{\partial} = \frac{a^2c^2}{(N\mathfrak{a})^2}$$

Anderseits ist

$$\begin{aligned} (a, b + c\omega)(a, b + c\omega') = \mathfrak{a}\mathfrak{a}' = N\mathfrak{a} \\ = \big(a^2, aS(b + c\omega), N(b + c\omega)\big) \end{aligned}$$

und daher der wegzudividierende Teiler in der Gleichung für α gerade $N\mathfrak{a}$, also in der Diskriminante von α genau $(N\mathfrak{a})^2$; es wird also II, 174

$$\begin{aligned} \mathsf{D} = \frac{a^2c^2d}{N\mathfrak{a}^2} = \boldsymbol{\partial}d = m^2d, \\ \boldsymbol{\partial} = m^2. \end{aligned}$$

Man sieht also, daß für die aus den Kettenbruchentwicklungen reduzierter Zahlen resultierenden Einheiten nicht nur die Modulklasse, sondern sogar deren Diskriminante $\boldsymbol{\partial} = m^2$ die Invariante ist:

Satz 26. *Die durch Kettenbruchentwicklung resultierenden Einheiten sind nur von der Diskriminante $\boldsymbol{\partial} = m^2$ der benutzten Modulklasse abhängig. Alle Basisquotienten aus Modulklassen der Diskriminante $\boldsymbol{\partial} = m^2$ liefern die Einheiten von R_m .*

Beispiel.

$$d = 10\,, \quad \text{Modulklasse } (4, \sqrt{10})\,, \quad \alpha = \frac{\sqrt{10}}{4}$$

$$\mathsf{D} = 160 = 4d$$

$$\boldsymbol{\partial} = m^2 = 4\,; \quad m = 2.$$

$$\mathsf{R}_m = a + 2b\sqrt{10}$$

Kettenbruchentwicklung von $\alpha = \frac{\sqrt{10}}{4}$:

$$\begin{array}{rcll} \alpha &=& 0 + \frac{\sqrt{10}}{4} = 0 + \frac{1}{\alpha_1} & a_0 = 0 \\ \alpha_1 &=& \frac{4}{\sqrt{10}} = \frac{2\sqrt{10}}{5} = 1 + \frac{1}{\alpha_2} & a_1 = 1 \end{array}$$

II, 175

$$\begin{array}{rcll} \alpha_2 &=& \frac{5}{2\sqrt{10}-5} = \frac{2\sqrt{10}+5}{3} = 3 + \frac{1}{\alpha_3} & a_2 = 3 \\ \alpha_3 &=& \frac{3}{2\sqrt{10}-4} = \frac{\sqrt{10}+2}{4} = 1 + \frac{1}{\alpha_4} & a_3 = 1 \\ \alpha_4 &=& \frac{4}{\sqrt{10}-2} = \frac{2\sqrt{10}+4}{3} = 3 + \frac{1}{\alpha_5} & a_4 = 3 \\ \alpha_5 &=& \frac{3}{2\sqrt{10}-5} = \frac{2\sqrt{10}+5}{5} = 2 + \frac{1}{\alpha_6} & a_5 = 2 \\ \alpha_6 &=& \frac{5}{2\sqrt{10}-5} = \frac{2\sqrt{10}+5}{3} = \alpha_2 & a_6 = 3 \end{array}$$

Periode: $(3, 1, 3, 2)$, reduzierte Zahl $\alpha_2 = \frac{2\sqrt{10}+5}{3}$

Näherungsbrüche:

		3	1	3	2
0	1	3	4	15	34
1	0	1	1	4	9

$$\begin{array}{rclrcl} p_4 &=& 34 & p_3 &=& 15 \\ q_4 &=& 9 & q_3 &=& 4 \end{array}$$

$u = (9,\ 30,\ 15) = 3$ oder aus der Gleichung für $\alpha_2 = \frac{2\sqrt{10}+5}{3}$: $9x^2 - 30x = 15$ d. h. $3x^2 - 10x - 5 = 0$

$$u = \frac{9}{3} = 3$$
$$t = 38$$
$$38^2 - 3^2 \cdot 160 = 4$$
$$\eta = \frac{38 + 3\sqrt{160}}{2} = 19 + 6\sqrt{10}\,.$$

Tatsächlich ist die Grundeinheit von $\mathsf{R}(\sqrt{10})$

$$\varepsilon = 3 + \sqrt{10}\,.$$

Diese ist noch nicht in $\mathsf{R}_m = \mathsf{R}_2$ enthalten, wohl aber $\varepsilon^2 = 19 + 6\sqrt{10} = \eta$. II, 176

f.) Andere Methode zur Gewinnung von Einheiten.

Nach dem bisherigen kann die Aufgabe, die Grundeinheit von R_m zu finden, stets so gelöst werden, daß man den Basisquotienten eines Moduls der Diskriminante $\boldsymbol{\partial} = m^2$ aus $\mathsf{R}(\sqrt{d})$ in einen Kettenbruch entwickelt, und mit den Näherungsbrüchen der reinen Periode (reduzierten Zahl) des Verfahrens von Satz 17 anwendet. Als Modul der Diskriminante m^2 kann man etwa $\mathfrak{M} = (1, m\omega)$ nehmen, wenn $(1, \omega)$ eine Körperbasis von $\mathsf{R}(\sqrt{d})$ ist.

Es gibt noch eine andere, bequemere Methode, nämlich von der Kettenbruchentwicklung einer reinen Wurzel $\sqrt{\overline{\mathsf{D}}}$ auszugehen, deren Diskriminante sich aus der zugehörigen Gleichung

$$x^2 - \overline{\mathsf{D}} = 0$$

zu

$$\mathsf{D} = 4\overline{\mathsf{D}}$$

berechnet, wenn $\overline{\mathsf{D}}$ als ganze Zahl vorausgesetzt wird, die keine Quadratzahl ist.

Die Kettenbruchentwicklung von $+\sqrt{\overline{\mathsf{D}}}$ hat nach Satz 11 die Gestalt:

$$\sqrt{\overline{\mathsf{D}}} = (a_0;\ a_1, \ldots\ a_{n-1}, 2a_0;\ \ldots\ldots)$$

Es seien $\frac{\mathsf{P}_0}{\mathsf{Q}_0}, \ldots$ ihre Näherungsbrüche. Aus II, 177

$$\sqrt{\mathsf{D}} = \left(a_0;\, a_1, \dots\, a_{n-1}, a_0 + \sqrt{\mathsf{D}}\right)$$

folgt:

$$\sqrt{\mathsf{D}} = \frac{\left(a_0 + \sqrt{\mathsf{D}}\right)\mathsf{P}_{n-1} + \mathsf{P}_{n-2}}{\left(a_0 + \sqrt{\mathsf{D}}\right)\mathsf{Q}_{n-1} + \mathsf{Q}_{n-2}}$$

also

$$\begin{aligned} a_0\mathsf{Q}_{n-1} + \mathsf{Q}_{n-2} - \mathsf{P}_{n-1} &= 0 \\ \mathsf{D}\mathsf{Q}_{n-1} - a_0\mathsf{P}_{n-1} - \mathsf{P}_{n-2} &= 0 \end{aligned}$$

oder

$$\begin{aligned} \mathsf{Q}_{n-2} &= -a_0\mathsf{Q}_{n-1} + \mathsf{P}_{n-1} \\ \mathsf{P}_{n-2} &= \mathsf{D}\mathsf{Q}_{n-1} - a_0\mathsf{P}_{n-1}\,. \end{aligned}$$

Nun ist

$$\begin{vmatrix} \mathsf{P}_{n-1}\,, & \mathsf{P}_{n-2} \\ \mathsf{Q}_{n-1}\,, & \mathsf{Q}_{n-2} \end{vmatrix} = (-1)^n$$

Also folgt:

$$\begin{vmatrix} \mathsf{P}_{n-1} & \mathsf{D}\mathsf{Q}_{n-1} - a_0\mathsf{P}_{n-1} \\ \mathsf{Q}_{n-1} & \mathsf{P}_{n-1} - a_0\mathsf{Q}_{n-1} \end{vmatrix} = (-1)^n,$$

$$\mathsf{P}_{n-1}^2 - \mathsf{D}\mathsf{Q}_{n-1}^2 = (-1)^n.$$

Es resultiert also die Einheit:

$$\varepsilon = \mathsf{P}_{n-1} + \mathsf{Q}_{n-1}\sqrt{\mathsf{D}} = \frac{2\mathsf{P}_{n-1} + \mathsf{Q}_{n-1}\sqrt{\mathsf{D}}}{2}\,.$$

Wir wollen nun nachweisen, daß dies genau dieselbe Einheit ist, wie die aus $\sqrt{\mathsf{D}}$ nach der früheren Methode zu gewinnende. Dazu haben wir nur die reine Periode $(a_1, \dots\, a_{n-1}, 2a_0)$ zu benutzen, deren Näherungsbrüche wir mit $\frac{p_1}{q_1}, \dots$ bezeichnen. Zu ihr gehört

II, 178

$$\alpha = \frac{1}{\sqrt{\mathsf{D}} - a_0}$$

mit der Gleichung

$$(\mathsf{D} - a_0^2)x^2 - 2a_0 x - 1 = 0$$

Zwischen den $\frac{\mathsf{P}_\nu}{\mathsf{Q}_\nu}$ und $\frac{p_\nu}{q_\nu}$ bestehen die Beziehungen:

$$\frac{\mathsf{P}_\nu}{\mathsf{Q}_\nu} = a_0 + \frac{1}{\frac{p_\nu}{q_\nu}} = \frac{q_\nu + a_0 p_\nu}{p_\nu}$$

und daher

$$\left.\begin{aligned} \mathsf{P}_\nu &= q_\nu + a_0 p_\nu \\ \mathsf{Q}_\nu &= \quad p_\nu \end{aligned}\right\} \quad (\nu = 1, 2, \dots)$$

Speziell wird daher:

$$\begin{aligned} p_{n-1} &= \mathsf{Q}_{n-1} \\ q_{n-1} &= \mathsf{P}_{n-1} - a_0\mathsf{Q}_{n-1} \end{aligned}$$

$$\begin{aligned} p_{n-2} = \mathsf{Q}_{n-2} &= -a_0\mathsf{Q}_{n-1} + \mathsf{P}_{n-1} \\ q_{n-2} = \mathsf{P}_{n-2} - a_0\mathsf{Q}_{n-2} &= \overline{\mathsf{D}}\mathsf{Q}_{n-1} - a_0\mathsf{P}_{n-1} + a_0^2\mathsf{Q}_{n-1} - a_0\mathsf{P}_{n-1} \\ &= (\overline{\mathsf{D}} + a_0^2)\mathsf{Q}_{n-1} - 2a_0\mathsf{P}_{n-1} \end{aligned}$$

$$\begin{aligned} p_n = 2a_0 p_{n-1} + p_{n-2} &= 2a_0\mathsf{Q}_{n-1} - a_0\mathsf{Q}_{n-1} + \mathsf{P}_{n-1} = a_0\mathsf{Q}_{n-1} + \mathsf{P}_{n-1} \\ q_n = 2a_0 q_{n-1} + q_{n-2} &= 2a_0\mathsf{P}_{n-1} - 2a_0^2\mathsf{Q}_{n-1} + (\overline{\mathsf{D}} + a_0^2)\mathsf{Q}_{n-1} - 2a_0\mathsf{P}_{n-1} \\ &= (\overline{\mathsf{D}} - a_0^2)\mathsf{Q}_{n-1} \end{aligned}$$

Damit wird die nach dem früheren Verfahren zu konstruierende Lösung: II, 179

$$u = \frac{q_n}{\mathsf{D} - a_0^2} = \mathsf{Q}_{n-1}$$

$$t = p_n + q_{n-1} = 2\mathsf{P}_{n-1}$$

also

$$t^2 - \mathsf{D}u^2 = (2\mathsf{P}_{n-1})^2 - 4\overline{\mathsf{D}}\mathsf{Q}_{n-1}^2 = (-1)^n \cdot 4$$

$$\varepsilon = \frac{2\mathsf{P}_{n-1} + \mathsf{Q}_{n-1}\sqrt{\mathsf{D}}}{2}, \qquad \text{w. z. b. w.}$$

Um daher die Grundeinheit von R_m in $\mathsf{R}(\sqrt{d})$ zu finden, kann man auch so vorgehen:

$$\text{a.)}\ d \equiv 0 \mod 4.$$

Man unterscheide $\sqrt{\overline{\mathsf{D}}} = \sqrt{m^2 \frac{d}{4}}$. Dann ist $\mathsf{D} = m^2 d$.

$$\text{b.)}\ d \equiv 1 \mod 4.$$

Hier klappt das Verfahren nur für $m = 2m_0$, indem man dann

$$\sqrt{\overline{\mathsf{D}}} = \sqrt{\frac{m^2}{4} d} = \sqrt{m_0^2 d} \quad \text{mit} \quad \mathsf{D} = m^2 d$$

entwickelt.

Umgekehrt sei $\overline{\mathsf{D}} = \overline{m}^2 d_0$ und d_0 quadratfrei. Ist dann

$$\text{a.)}\ d_0 \equiv 2, 3 \mod 4,$$

so liefert die Entwicklung die Grundeinheit von $\mathsf{R}_{\overline{m}}$.

$$\text{b.)}\ d_0 \equiv 1 \mod 4,$$

so liefert die Entwicklung die Grundeinheit von $\mathsf{R}_{2\overline{m}}$.

Satz 27. Ist $\overline{\mathsf{D}}$ eine ganze, nicht quadratische, positive Zahl, so erhält man eine Lösung von II, 180

$$t^2 - \overline{\mathsf{D}}u^2 = \pm 1$$

indem man für t, u Zähler und Nenner des vorletzten Näherungsbruches vor Wiederkehr der Periode aus der Kettenbruchentwicklung von $\sqrt{\overline{\mathsf{D}}}$ nimmt, speziell die kleinste Lösung bei der primitiven Periode. Die so gelieferten Einheiten sind mit dem nach dem Verfahren von Satz 17 aus der reinperiodischen Entwicklung der zu $\sqrt{\overline{\mathsf{D}}}$ gehörigen reduzierten Zahlen identisch. Ist daher

$$\overline{\mathsf{D}} = \overline{m}^2 d_0$$

und d_0 quadratfrei, so resultiert für

$$\text{a.) } d_0 \equiv 2, 3 \mod 4\,;\ (d = 4d_0)$$

die Grundeinheit von $\mathsf{R}_{\overline{m}}$,

$$\text{b.) } d_0 \equiv 1 \mod 4\,;\ (d = d_0)$$

die Grundeinheit von $\mathsf{R}_{2\overline{m}}$.

Umgekehrt kann man also für $d \equiv 0 \mod 4$ die Grundeinheiten aller R_m durch Entwicklung von $\sqrt{m^2 \frac{d}{4}}$ erhalten, für $d \equiv 1 \mod 4$ auf diesem Wege jedoch nur die Grundeinheiten der R_{2m_0} durch Entwicklung von $\sqrt{m_0^2 d}$.

Anmerkung: Nach der bei Töplitz entstandenen Dissertation von Hansen besteht ein ähnliches Gesetz auch für $\frac{1+\sqrt{\mathsf{D}}}{2}$ falls $\mathsf{D} \equiv 1 \mod 4$. Dadurch vervollkommnet sich die Methode von Satz 27 auf alle überhaupt vorkommenden Einheiten.

2.2 Jacobi–Algorithmen in kubischen Körpern. (Dez. 1923)

After having presented the classical theory of continued fraction expansions of quadratic irrationals, Hasse now works through Perron's work [Per07], *which deals with continued fractions of cubic irrationals. In section f.)] he refers to a conversation with Toeplitz. Hasse returns to this topic later in his papers* [BH65, BH69, EH67].

II, 181

Dezember 1923.

a.) Das Formale, erläutert durch Gegenüberstellung der zwei– und dreigliedrigen Algorithmen.

$k = 2$.

Gegeben seien zwei reelle Zahlen x_0, x_1. Wir betrachten folgenden Algorithmus ($x_0 > 0$):

$$\begin{array}{ll}
x_1 = a_1^{(0)} x_0 + x_0^{(1)}; & x_0 = x_1^{(1)} \\
x_1^{(1)} = a_1^{(1)} x_0^{(1)} + x_0^{(2)}; & x_0^{(1)} = x_1^{(2)} \\
x_1^{(2)} = a_1^{(2)} x_0^{(2)} + x_0^{(3)}; & x_0^{(2)} = x_1^{(3)} \\
\cdots\cdots\cdots & \cdots\cdots \\
x_1^{(\nu)} = a_1^{(\nu)} x_0^{(\nu)} + x_0^{(\nu+1)}; & x_0^{(\nu)} = x_1^{(\nu+1)} \\
\cdots\cdots\cdots & \cdots\cdots
\end{array}$$

kurz :

$$\begin{array}{ccc}
x_0 & & x_1 \\
& a_1^{(0)} & \\
x_0^{(1)} & & x_1^{(1)} \\
& a_1^{(1)} & \\
x_0^{(2)} & & x_1^{(2)} \\
\cdots & \cdots & \cdots \\
x_0^{(\nu)} & & x_1^{(\nu)} \\
& a_1^{(\nu)} & \\
x_0^{(\nu+1)} & & x_1^{(\nu+1)} \\
\cdots & \cdots & \cdots
\end{array}$$

wo stets $a_1^{(\nu)}$ das größte Ganze in $\frac{x_1^{(\nu)}}{x_0^{(\nu)}}$ ist.

Dieser Algorithmus bedeutet matrizentheoretisch:

$$\left(x_0^{(\nu)}, \quad x_1^{(\nu)}\right) = \begin{pmatrix} 0 & 1 \\ 1 & a_1^{(\nu)} \end{pmatrix} \left(x_0^{(\nu+1)}, \quad x_1^{(\nu+1)}\right)$$

Zwei aufeinanderfolgende Zeilen des rechtsstehenden Schemas hängen also ganzzahlig linear mit der Determinante -1 zusammen, oder sind kurz gesagt, *uneigentlich äquivalent.* II, 182

$k = 3.$

Gegeben seien drei reelle Zahlen x_0, x_1, x_2. Wir betrachten folgenden Algorithmus ($x_0 > 0$):

$$\begin{array}{lll}
x_1 = a_1^{(0)} x_0 + x_0^{(1)}; & x_2 = a_2^{(0)} x_0 + x_1^{(1)}; & x_0 = x_2^{(1)} \\
x_1^{(1)} = a_1^{(1)} x_0^{(1)} + x_0^{(2)}; & x_2^{(1)} = a_2^{(1)} x_0^{(1)} + x_1^{(2)}; & x_0^{(1)} = x_2^{(2)} \\
\dots\dots & \dots\dots & \dots\dots \\
x_1^{(\nu)} = a_1^{(\nu)} x_0^{(\nu)} + x_0^{(\nu+1)}; & x_2^{(\nu)} = a_2^{(\nu)} x_0^{(\nu)} + x_1^{(\nu+1)}; & x_0^{(\nu)} = x_2^{(\nu+1)}
\end{array}$$

kurz:

$$\begin{array}{ccccc}
x_0 & & x_1 & & x_2 \\
& a_1^{(0)} & & a_2^{(0)} & \\
x_0^{(1)} & & x_1^{(1)} & & x_2^{(1)} \\
& a_1^{(1)} & & a_2^{(1)} & \\
x_0^{(2)} & & x_1^{(2)} & & x_2^{(2)} \\
\dots & \dots & \dots & \dots & \dots \\
x_0^{(\nu)} & & x_1^{(\nu)} & & x_2^{(\nu)} \\
& a_1^{(\nu)} & & a_2^{(\nu)} & \\
x_0^{(\nu+1)} & & x_1^{(\nu+1)} & & x_2^{(\nu+1)} \\
\dots & \dots & \dots & \dots & \dots
\end{array}$$

wo stets $a_1^{(\nu)}, a_2^{(\nu)}$ die größten Ganzen in $\frac{x_1^{(\nu)}}{x_0^{(\nu)}}; \frac{x_2^{(\nu)}}{x_0^{(\nu)}}$ sind. Dieser Algorithmus bedeutet matrizentheoretisch:

$$\left(x_0^{(\nu)}, \quad x_1^{(\nu)}, \quad x_2^{(\nu)}\right) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & a_1^{(\nu)} \\ 0 & 1 & a_2^{(\nu)} \end{pmatrix} \left(x_0^{(\nu+1)}, \quad x_1^{(\nu+1)}, \quad x_2^{(\nu+1)}\right) .$$

Zwei aufeinanderfolgende Zeilen sind *eigentlich äquivalent.* II, 183

Mindestens von der zweiten Zeile an sind die $x_0^{(\nu)}, x_1^{(\nu)}$ positiv, die $a_1^{(\nu)}$ also auch. Für ganzzahlige x_0, x_1 führt daher der Algorithmus (hier mit dem

Euklidischen Teilerverfahren identisch), da die $x_0^{(\nu)}, x_1^{(\nu)}$ beständig abnehmen, schließlich einmal auf ein erstes $x_0^{(\nu+1)} = 0$, während noch $x_0^{(\nu)} = x_1^{(\nu+1)} \neq 0$ ist. Dann ist offenbar wegen der Äquivalenz von (x_0, x_1) mit $\left(x_0^{(\nu+1)}, x_1^{(\nu+1)}\right) = \left(0, x_1^{(\nu+1)}\right)$ $x_1^{(\nu+1)}$ der größte gemeinsame Teiler von x_0, x_1.

Sind aber x_0, x_1 linear unabhängig $\left(\frac{x_1}{x_0} \text{ irrational}\right)$, so kann niemals ein $x_0^{(\nu)}, x_1^{(\nu)}$ gleich Null werden, wegen der Äquivalenz. Der Algorithmus bricht also nicht ab.

Es ist vorteilhafter die Relation zwischen zwei aufeinanderfolgenden Zeilen so zu schreiben:

$$\left(x_1^{(\nu)}, \quad x_0^{(\nu)}\right) = \begin{pmatrix} a_1^{(\nu)} & 1 \\ 1 & 0 \end{pmatrix} \left(x_1^{(\nu+1)}, \quad x_0^{(\nu+1)}\right).$$

Hieraus folgt durch wiederholte Anwendung:

$$(x_1, \quad x_0) = \begin{pmatrix} a_1^{(0)} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1^{(1)} & 1 \\ 1 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} a_1^{(\nu)} & 1 \\ 1 & 0 \end{pmatrix} \left(x_1^{(\nu+1)}, \quad x_0^{(\nu+1)}\right).$$

Durch hintere Multiplikation mit $\begin{pmatrix} a_1^{(\nu)} & 1 \\ 1 & 0 \end{pmatrix}$ entsteht aus einer beliebigen 2 reihigen Matrix eine neue, die die erste Spalte der ursprünglichen zur zweiten Spalte hat. Daher kann man allgemein setzen

$$(x_1, \quad x_0) = \begin{pmatrix} \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{pmatrix} \left(x_1^{(\nu+1)}, \quad x_0^{(\nu+1)}\right)$$

II, 184

Mindestens von der zweiten Zeile an sind die $x_0^{(\nu)}, x_1^{(\nu)}, x_2^{(\nu)}$ positiv, also auch die $a_1^{(\nu)}, a_2^{(\nu)}$. Ferner sind dann offenbar stets $x_0^{(\nu+1)}, x_1^{(\nu+1)}$ kleiner als $x_0^{(\nu)} < x_0^{(\nu-1)}$ und auch $x_2^{(\nu+1)} = x_0^{(\nu)} < x_0^{(\nu-1)}$. Die obere Schranke $x_0^{(\nu-1)}$ für die $(\nu+1)$–te Zeile $\left(x_0^{(\nu+1)}, x_1^{(\nu+1)}, x_2^{(\nu+1)}\right)$ wird aber selbst stets kleiner. Für ganzzahlige x_0, x_1, x_2 wird daher sicher einmal eine Zeile mit mindestens einer Null erreicht, (und zwar notwendig zum erstenmal an erster oder zweiter Stelle). Damit ist dann die Bestimmung des größten gemeinsamen Teilers von x_0, x_1, x_2 auf die von 2 Zahlen zurückgeführt, die nach dem zweigliedrigen Algorithmus fortgesetzt werden kann.

Sind aber x_0, x_1, x_2 linear unabhängig ($x_0 : x_1 : x_2$ irrational), so kann wegen der Äquivalenz keine Zeile eine Null enthalten, der Algorithmus bricht also nie ab.

Vorteilhaftere Schreibweise:

$$\left(x_2^{(\nu)},\quad x_1^{(\nu)},\quad x_0^{(\nu)}\right) = \begin{pmatrix} a_2^{(\nu)} & 1 & 0 \\ a_1^{(\nu)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \left(x_2^{(\nu+1)},\quad x_1^{(\nu+1)},\quad x_0^{(\nu+1)}\right).$$

Relation zwischen 0–ter und $(\nu+1)$–ter Zeile:

$$\left(x_2,\quad x_1,\quad x_0\right) = \begin{pmatrix} a_2^{(0)} & 1 & 0 \\ a_1^{(0)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} a_2^{(\nu)} & 1 & 0 \\ a_1^{(\nu)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \left(x_2^{(\nu+1)}, x_1^{(\nu+1)}, x_0^{(\nu+1)}\right)$$

Allgemeiner Ansatz:

$$\left(x_2,\quad x_1,\quad x_0\right) = \begin{pmatrix} \mathsf{A}_2^{(\nu+3)} & \mathsf{A}_2^{(\nu+2)} & \mathsf{A}_2^{(\nu+1)} \\ \mathsf{A}_1^{(\nu+3)} & \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+3)} & \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{pmatrix} \left(x_2^{(\nu+1)},\quad x_1^{(\nu+1)},\quad x_0^{(\nu+1)}\right)$$

Dann besteht für die Größen $\mathsf{A}_i^{(\nu)}$ folgende *Rekursionsformel*: II, 185

$$\begin{pmatrix} \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{pmatrix} = \begin{pmatrix} \mathsf{A}_1^{(\nu+1)} & \mathsf{A}_1^{(\nu)} \\ \mathsf{A}_0^{(\nu+1)} & \mathsf{A}_0^{(\nu)} \end{pmatrix} \begin{pmatrix} a_1^{(\nu)} & 1 \\ 1 & 0 \end{pmatrix}$$

$$(\nu = 0, 1, 2, \dots)$$

Explizite Rekursionsformeln:

$$\begin{aligned} \mathsf{A}_1^{(\nu+2)} &= \mathsf{A}_1^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_1^{(\nu)} \\ \mathsf{A}_0^{(\nu+2)} &= \mathsf{A}_0^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_0^{(\nu)} \end{aligned}$$

Offenbar ist zu setzen: $\mathsf{A}_1^{(1)} = 1$; $\mathsf{A}_0^{(1)} = 0$, (man setze $\nu = 0$).
Ferner $(\nu = -1)$: $\mathsf{A}_1^{(0)} = 0$; $\mathsf{A}_0^{(1)} = 1$. Insgesamt:
Anfangsbedingung:

$$\begin{pmatrix} \mathsf{A}_1^{(1)} & \mathsf{A}_1^{(0)} \\ \mathsf{A}_0^{(1)} & \mathsf{A}_0^{(0)} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Hieraus entsteht folgendes *Rekursionsschema für die* $\mathsf{A}_i^{(\nu)}$:

			1	1	1
			$a_1^{(0)}$	$a_1^{(1)}$	$a_1^{(2)}$
$\mathsf{A}_1^{(\nu)}$	0	1	$a_1^{(0)}$	$a_1^{(1)}a_1^{(0)}+1$	$a_1^{(2)}a_1^{(1)}a_1^{(0)}+a_1^{(2)}+a_1^{(0)}$
$\mathsf{A}_0^{(\nu)}$	1	0	1	$a_1^{(1)}$	$a_1^{(2)}a_1^{(1)}+1$
$\nu =$	0	1	2	3	4

Determinantenbedingung:

$$\begin{vmatrix} \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{vmatrix} = (-1)^{\nu+1}$$

II, 186 *Rekursionsformel für die* $\mathsf{A}_i^{(\nu)}$:

$$\begin{pmatrix} \mathsf{A}_2^{(\nu+3)} & \mathsf{A}_2^{(\nu+2)} & \mathsf{A}_2^{(\nu+1)} \\ \mathsf{A}_1^{(\nu+3)} & \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+3)} & \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{pmatrix} = \begin{pmatrix} \mathsf{A}_2^{(\nu+2)} & \mathsf{A}_2^{(\nu+1)} & \mathsf{A}_2^{(\nu)} \\ \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} & \mathsf{A}_1^{(\nu)} \\ \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} & \mathsf{A}_0^{(\nu)} \end{pmatrix} \begin{pmatrix} a_2^{(\nu)} & 1 & 0 \\ a_1^{(\nu)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

$$(\nu = 0, 1, 2, \dots)$$

Explizite Rekursionsformeln:

$$\begin{aligned} \mathsf{A}_2^{(\nu+3)} &= \mathsf{A}_2^{(\nu+2)} a_2^{(\nu)} + \mathsf{A}_2^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_2^{(\nu)} \\ \mathsf{A}_1^{(\nu+3)} &= \mathsf{A}_1^{(\nu+2)} a_2^{(\nu)} + \mathsf{A}_1^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_1^{(\nu)} \\ \mathsf{A}_0^{(\nu+3)} &= \mathsf{A}_0^{(\nu+2)} a_2^{(\nu)} + \mathsf{A}_0^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_0^{(\nu)} . \end{aligned}$$

Analog folgt als *Anfangsbedingung*:

$$\begin{pmatrix} \mathsf{A}_2^{(2)} & \mathsf{A}_2^{(1)} & \mathsf{A}_2^{(0)} \\ \mathsf{A}_1^{(2)} & \mathsf{A}_1^{(1)} & \mathsf{A}_1^{(0)} \\ \mathsf{A}_0^{(2)} & \mathsf{A}_0^{(1)} & \mathsf{A}_0^{(0)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} .$$

Berechnungsschema für die $\mathsf{A}_i^{(\nu)}$:

				1	1	1
				$a_1^{(0)}$	$a_1^{(1)}$	$a_1^{(2)}$
				$a_2^{(0)}$	$a_2^{(1)}$	$a_2^{(2)}$
$\mathsf{A}_2^{(\nu)}$	0	0	1	$a_2^{(0)}$	$a_2^{(1)}a_2^{(0)}+a_1^{(1)}$	$a_2^{(2)}a_2^{(1)}a_2^{(0)}+a_2^{(2)}a_1^{(1)}+a_1^{(2)}a_2^{(0)}+1$
$\mathsf{A}_1^{(\nu)}$	0	1	0	$a_1^{(0)}$	$a_2^{(1)}a_1^{(0)}+1$	$a_2^{(2)}a_2^{(1)}a_1^{(0)}+a_2^{(2)}+a_1^{(2)}a_1^{(0)}$
$\mathsf{A}_0^{(\nu)}$	1	0	0	1	$a_2^{(1)}$	$a_2^{(2)}a_2^{(1)}+a_1^{(2)}$
$\nu=$	0	1	2	3	4	5

Determinantenbedingung:

$$\begin{vmatrix} \mathsf{A}_2^{(\nu+3)} & \mathsf{A}_2^{(\nu+2)} & \mathsf{A}_2^{(\nu+1)} \\ \mathsf{A}_1^{(\nu+3)} & \mathsf{A}_1^{(\nu+2)} & \mathsf{A}_1^{(\nu+1)} \\ \mathsf{A}_0^{(\nu+3)} & \mathsf{A}_0^{(\nu+2)} & \mathsf{A}_0^{(\nu+1)} \end{vmatrix} = 1$$

II, 187

b.) Konvergenzbeweis für den Jacobi–Algorithmus.

Ich beweise folgenden

Satz 1. *Sind x_0, x_1, x_2 drei linear unabhängige reelle Zahlen, so konvergieren die Verhältnisse $\mathsf{A}_0^{(\nu)} : \mathsf{A}_1^{(\nu)} : \mathsf{A}_2^{(\nu)}$ der Näherungswerte des Jacobi–Algorithmus von x_0, x_1, x_2 gegen das Verhältnis $x_0 : x_1 : x_2$.*

Bemerkung: „Linear unabhängig“ soll hier wie im Folgenden stets bedeuten, daß keine ganzzahlige lineare, homogene Relation $m_0x_0+m_1x_1+m_2x_2=0$ besteht. Dies ist hinreichend dafür, daß der Jacobi–Algorithmus nie abbricht.

Beweis: Wie wir früher sahen, sind von mindestens der zweiten Zeile an die auftretenden Restetripel $x_0^{(\nu)}, x_1^{(\nu)}, x_2^{(\nu)}$ als auch die $a_1^{(\nu)}, a_2^{(\nu)} \geqq 0$. Wir können uns daher auf den Fall positiver x_0, x_1, x_2 und von vornherein positiver $a_1^{(\nu)}, a_2^{(\nu)}$ beschränken. Denn die Reihe der Näherungswerte $\mathsf{A}_0^{(\nu)}, \mathsf{A}_1^{(\nu)}, \mathsf{A}_2^{(\nu)}$ des Algorithmus für x_0, x_1, x_2 hängt mit den Näherungswerten $\mathsf{B}_0^{(\nu-\kappa)}, \mathsf{B}_1^{(\nu-\kappa)}, \mathsf{B}_2^{(\nu-\kappa)}$ des Algorithmus von y_0, y_1, y_2 durch dieselbe lineare Substitution S zusammen, durch die y_0, y_1, y_2 mit x_0, x_1, x_2 zusammenhängt, wenn x_0, x_1, x_2 die κ-ten Reste des Algorithmus von y_0, y_1, y_2 sind. Gilt also

II, 188

$$\lim_{\nu=\infty} \mathsf{A}_0^{(\nu)} : \mathsf{A}_1^{(\nu)} : \mathsf{A}_2^{(\nu)} = x_0 : x_1 : x_2$$

so gilt wegen

$$\left(\mathsf{B}_0^{(\nu-\kappa)}, \mathsf{B}_1^{(\nu-\kappa)}, \mathsf{B}_2^{(\nu-\kappa)}\right) = \mathsf{S}\left(\mathsf{A}_0^{(\nu)}, \mathsf{A}_1^{(\nu)}, \mathsf{A}_2^{(\nu)}\right)$$

und

$$(y_0, y_1, y_2) = \mathsf{S}\,(x_0 : x_1 : x_2)$$

auch

$$\lim_{n=\infty} \mathsf{B}_0^{(\nu-\kappa)} : \mathsf{B}_1^{(\nu-\kappa)} : \mathsf{B}_2^{(\nu-\kappa)} = y_0 : y_1 : y_2 \,.$$

Wir nehmen also jetzt an:

$$x_0, x_1, x_2 > 0\,; \quad a_1^{(\nu)}, a_2^{(\nu)} \geqq 0\,; \quad (\nu = 0, 1, 2, \dots).$$

Wir brauchen dann noch folgende beiden Aussagen über die $a_1^{(\nu)}, a_2^{(\nu)}$, die stets angenommen werden dürfen:

I. Es ist stets $a_2^{(\nu)} \geqq 1\,;$ $\quad(\nu = 0, 1, 2, \dots)$

II. Es ist stets $0 \leqq a_1^{(\nu)} \leqq a_2^{(\nu)};$ $\quad(\nu = 0, 1, 2, \dots)$

I. folgt aus den Gleichungen, die die $a_2^{(\nu)}$ definieren, nämlich

$$x_2^{(\nu)} = a_2^{(\nu)} x_0^{(\nu)} + x_1^{(\nu+1)},$$

wonach $a_2^{(\nu)}$ als größtes Ganze von $\frac{x_2^{(\nu)}}{x_0^{(\nu)}} = \frac{x_0^{(\nu-1)}}{x_0^{(\nu)}}$ definiert ist. Nun ist für $\nu \geqq 1$ wegen

$$x_1^{(\nu-1)} = a_1^{(\nu-1)} x_0^{(\nu-1)} + x_0^{(\nu)}$$

$x_0^{(\nu)}$ als Rest mod. $x_0^{(\nu-1)}$ sicher $< x_0^{(\nu-1)}$, also $\frac{x_0^{(\nu-1)}}{x_0^{(\nu)}} > 1$, und somit für $\nu \geqq 1$ I. bewiesen. Da es aber auf Weglassen einer Anfangszeile nicht ankommt, darf I. schon für $\nu \geqq 0$ angenommen werden. II. folgt ebenso aus den Gleichungen

II, 189

$$x_1^{(\nu)} = a_1^{(\nu)} x_0^{(\nu)} + x_0^{(\nu+1)}; \quad x_2^{(\nu)} = a_2^{(\nu)} x_0^{(\nu)} + x_1^{(\nu+1)},$$

wonach $a_1^{(\nu)}$ als größtes Ganze von $\frac{x_1^{(\nu)}}{x_0^{(\nu)}}$ sicher nicht größer ist als das größte Ganze $a_2^{(\nu)}$ von $\frac{x_2^{(\nu)}}{x_0^{(\nu)}} = \frac{x_0^{(\nu+1)}}{x_0^{(\nu)}}$, weil ja wegen (für $\nu \geqq 1$):

$$x_2^{(\nu-1)} = a_2^{(\nu-1)} x_0^{(\nu-1)} + x_1^{(\nu)}$$

sicher $x_1^{(\nu)} < x_0^{(\nu-1)}$ ist. Damit ist II. für $\nu \geqq 1$ bewiesen, und es darf seine Richtigkeit schon für $\nu \geqq 0$ angenommen werden.

Wir betrachten nunmehr die Näherungswerte $\mathsf{A}_i^{(\nu)}$, definiert durch die obigen Rekursionsformeln. Wegen $\mathsf{A}_0^{(3)} = 1$ und

$$\mathsf{A}_0^{(\nu+3)} = \mathsf{A}_0^{(\nu+2)} a_2^{(\nu)} + \mathsf{A}_0^{(\nu+1)} a_1^{(\nu)} + \mathsf{A}_0^{(\nu)}; \quad (\nu \geqq 0)$$

sowie

$$a_2^{(\nu)} \geqq 1 \quad \text{für } \nu \geqq 0,$$

ist sicherlich

$$1 \leqq \mathsf{A}_0^{(\nu)} < \mathsf{A}_0^{(\nu+1)} < \cdots\cdots \quad (\text{für } \nu \geqq 3),$$

also speziell alle $\mathsf{A}_0^{(\nu)}$ von $\mathsf{A}_0^{(3)}$ an $\neq 0$ und sogar positiv. (Ebenso sind übrigens alle $\mathsf{A}_i^{(\nu)}$ für $\nu \geqq 4$ positiv und monoton wachsend, oder jedenfalls nicht abnehmend).

Wir betrachten für $\nu \geqq 4$ die 3 Quotienten

$$\frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}}, \frac{\mathsf{A}_i^{(\nu+1)}}{\mathsf{A}_0^{(\nu)}}, \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu)}}; \quad (\text{für } i = 1 \text{ oder } 2),$$

die wegen $\mathsf{A}_0^{(\nu)} > 0$ endliche, positive Zahlen sind. Die kleinste unter ihnen sei $\beta_i^{(\nu)}$, die größte $\mathsf{B}_i^{(\nu)}$, sodaß II, 190

$$\beta_i^{(\nu)} \leqq \mathsf{B}_i^{(\nu)}.$$

Nun ist ($\nu \geqq 4$):

$$\begin{aligned}\frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} &= \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} \cdot \frac{\mathsf{A}_0^{(\nu+2)}}{\mathsf{A}_0^{(\nu+3)}} \cdot a_2^{(\nu)} + \frac{\mathsf{A}_i^{(\nu+1)}}{\mathsf{A}_0^{(\nu+1)}} \cdot \frac{\mathsf{A}_0^{(\nu+1)}}{\mathsf{A}_0^{(\nu+3)}} \cdot a_1^{(\nu)} + \\ &\qquad + \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} \cdot \frac{\mathsf{A}_0^{(\nu)}}{\mathsf{A}_0^{(\nu+3)}} \\ &= \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} \lambda_2^{(\nu)} + \frac{\mathsf{A}_i^{(\nu+1)}}{\mathsf{A}_0^{(\nu+1)}} \lambda_1^{(\nu)} + \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} \lambda_0^{(\nu)},\end{aligned}$$

wo $\lambda_2^{(\nu)}, \lambda_1^{(\nu)}, \lambda_0^{(\nu)}$ die ersichtliche Bedeutung haben und nach den Rekursionsformeln

$$\lambda_2^{(\nu)} + \lambda_1^{(\nu)} + \lambda_0^{(\nu)} = 1,$$

ferner offenbar $\lambda_\kappa^{(\nu)} \geqq 0$ ist.

Nach Definition von $\beta_i^{(\nu)}, \mathsf{B}_i^{(\nu)}$ folgt also

$$\begin{aligned}\frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} &\leqq \left(\lambda_2^{(\nu)} + \lambda_1^{(\nu)} + \lambda_0^{(\nu)}\right) \mathsf{B}_i^{(\nu)} = \mathsf{B}_i^{(\nu)} \\ \frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} &\geqq \left(\lambda_2^{(\nu)} + \lambda_1^{(\nu)} + \lambda_0^{(\nu)}\right) \beta_i^{(\nu)} = \beta_i^{(\nu)},\end{aligned}$$

also sicher

$$\begin{aligned}\mathsf{B}_i^{(\nu+1)} &\leqq \mathsf{B}_i^{(\nu)}, \\ \beta_i^{(\nu+1)} &\leqq \beta_i^{(\nu)}.\end{aligned}$$

Daher gilt

$$0 \leqq \beta_i^{(\nu)} \leqq \beta_i^{(\nu+1)} \leqq \cdots\cdots \leqq \mathsf{B}_i^{(\nu+1)} \leqq \mathsf{B}_i^{(\nu)}.$$

Bekanntlich folgt hieraus die Konvergenz sowohl der $\beta_i^{(\nu)}$, als auch der $\mathsf{B}_i^{(\nu)}$ gegen eine obere bezw. untere Grenze β_i bezw. B_i. Unsere Behauptung ist dann

II, 191

$$\beta_i = \mathsf{B}_i \quad (\text{für } i = 1, 2),$$

woraus leicht auf

$$\lim_{\nu=\infty} \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} = \beta_i = \mathsf{B}_i$$

zu schließen ist.

Nehmen wir an es sei $\beta_i < \mathsf{B}_i$, was offenbar wegen

$$0 \leqq \beta_i^{(\nu)} \leqq \beta_i \leqq \mathsf{B}_i \leqq \mathsf{B}_i^{(\nu)}$$

neben $\beta_i = \mathsf{B}_i$ der einzig mögliche Fall ist. Für hinreichend hohes $\nu \geqq \nu_0$ kann dann $\beta_i - \beta_i^{(\nu)} = \varepsilon$ beliebig klein gemacht werden, und es ist dann also

$$\frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} \geqq \beta_i^{(\nu)} = \beta_i - \varepsilon.$$

Daraus folgt:

$$\begin{aligned} \frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} &\geqq \left(\lambda_1^{(\nu)} + \lambda_0^{(\nu)}\right) \beta_i^{(\nu)} + \lambda_2^{(\nu)} \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} \\ &= \left(1 - \lambda_2^{(\nu)}\right) (\beta_i - \varepsilon) + \lambda_2^{(\nu)} \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}}, \end{aligned}$$

also

$$\frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} - \beta_i \geqq \lambda_2^{(\nu)} \left(\frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} - \beta_i \right) - \varepsilon .$$

Nun folgt aus

$$a_2^{(\nu)} \geqq a_1^{(\nu)} \geqq 0 ; \quad a_2^{(\nu)} \geqq 1$$

und

$$\mathsf{A}_0^{(\nu+2)} > \mathsf{A}_0^{(\nu)}; \quad \mathsf{A}_0^{(\nu+2)} > \mathsf{A}_0^{(\nu+1)}$$

daß

$$\lambda_2^{(\nu)} > \lambda_1^{(\nu)}; \quad \lambda_2^{(\nu)} > \lambda_0^{(\nu)},$$

also wegen

$$1 = \lambda_2^{(\nu)} + \lambda_1^{(\nu)} + \lambda_0^{(\nu)},$$

daß

II, 192

$$1 < 3\lambda_2^{(\nu)},$$

also

$$\lambda_2^{(\nu)} > \frac{1}{3}$$

ist. Daraus folgt für $\nu \geqq \nu_0$

$$\frac{\mathsf{A}_i^{(\nu+3)}}{\mathsf{A}_0^{(\nu+3)}} - \beta_i > \frac{1}{3}\left(\frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} - \beta_i\right) - \varepsilon,$$

also durch κ malige Anwendung:

$$\frac{\mathsf{A}_i^{(\nu+2+\kappa)}}{\mathsf{A}_0^{(\nu+2+\kappa)}} - \beta_i > \frac{1}{3^\kappa}\left(\frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} - \beta_i\right) - \varepsilon\left(1 + \frac{1}{3} + \cdots + \frac{1}{3^{\kappa-1}}\right).$$

Ich denke mir nun ν so gewählt, daß $\frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}}$ gerade der betreffende $\mathsf{B}_i^{(\mu)}$ wird, was stets möglich, da unter 3 aufeinanderfolgenden solchen Quotienten mindestens einer (nämlich der größte) ein $\mathsf{B}_i^{(\mu)}$ ist. Es ist dann

$$\frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} = \mathsf{B}_i^{(\mu)} \geqq \mathsf{B}_i\,.$$

Ferner ist dann unter den $\frac{\mathsf{A}_i^{(\nu+2+\kappa)}}{\mathsf{A}_0^{(\nu+2+\kappa)}}$ für $\kappa = 1, 2, 3$ sicher eins ein $\beta_i^{(\mu)}$, also $\leqq \beta_i$. So soll κ bestimmt sein. Dann folgt für dieses ν und κ:

$$0 \geqq \frac{\mathsf{A}_i^{(\nu+2+\kappa)}}{\mathsf{A}_0^{(\nu+2+\kappa)}} - \beta_i > \frac{1}{3^\kappa}(\mathsf{B}_i - \beta_i) - \varepsilon\left(1 + \frac{1}{3} + \cdots + \frac{1}{3^{\kappa-1}}\right)$$

Durch hinreichend kleine Wahl von ε käme also für $\mathsf{B}_i > \beta_i$ ein Widerspruch heraus. Es ist somit $\beta_i = \mathsf{B}_i$ und daher $\lim_{\nu=\infty} \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}}$ vorhanden. II, 193

Es ist nun letztens noch zu zeigen, daß der vorhandene

$$\lim_{\nu=\infty} \mathsf{A}_2^{(\nu)} : \mathsf{A}_1^{(\nu)} : \mathsf{A}_0^{(\nu)} = x_2 : x_1 : x_0$$

ist. Dazu benutzen wir die Formeln:

$$\begin{aligned} x_2 &= \mathsf{A}_2^{(\nu+2)} x_2^{(\nu)} + \mathsf{A}_1^{(\nu+1)} x_1^{(\nu)} + \mathsf{A}_2^{(\nu)} x_0^{(\nu)} \\ x_1 &= \mathsf{A}_1^{(\nu+2)} x_2^{(\nu)} + \mathsf{A}_1^{(\nu+1)} x_1^{(\nu)} + \mathsf{A}_1^{(\nu)} x_0^{(\nu)} \\ x_0 &= \mathsf{A}_0^{(\nu+2)} x_2^{(\nu)} + \mathsf{A}_0^{(\nu+1)} x_1^{(\nu)} + \mathsf{A}_0^{(\nu)} x_0^{(\nu)} \end{aligned}$$

und zwar in der inhomogenen Gestalt:

$$\frac{x_i}{x_0} = \frac{\mathsf{A}_i^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}} + \mathsf{A}_i^{(\nu+1)} \frac{x_1^{(\nu)}}{x_0^{(\nu)}} + \mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}} + \mathsf{A}_0^{(\nu+1)} \frac{x_1^{(\nu)}}{x_0^{(\nu)}} + \mathsf{A}_0^{(\nu)}}; \quad (i = 1, 2).$$

oder

$$\begin{aligned} \frac{x_i}{x_0} &= \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} \cdot \frac{\mathsf{A}_0^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}}}{\mathsf{A}_0^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}} + \cdots} + \frac{\mathsf{A}_i^{(\nu+1)}}{\mathsf{A}_0^{(\nu+1)}} \cdot \frac{\mathsf{A}_0^{(\nu+1)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}}}{\mathsf{A}_0^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}} + \cdots} \\ &\quad + \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} \cdot \frac{\mathsf{A}_0^{(\nu)}}{\mathsf{A}_0^{(\nu+2)} \frac{x_2^{(\nu)}}{x_0^{(\nu)}} + \cdots} \\ &= \frac{\mathsf{A}_i^{(\nu+2)}}{\mathsf{A}_0^{(\nu+2)}} \kappa_2^{(\nu)} + \frac{\mathsf{A}_i^{(\nu+1)}}{\mathsf{A}_0^{(\nu+1)}} \kappa_1^{(\nu)} + \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} \kappa_0^{(\nu)}, \end{aligned}$$

wo $\kappa_2^{(\nu)} + \kappa_1^{(\nu)} + \kappa_0^{(\nu)} = 1$, und

$$\kappa_2^{(\nu)}, \kappa_1^{(\nu)}, \kappa_0^{(\nu)} > 0.$$

Hieraus folgt wegen $\lim\limits_{\nu=\infty} \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}} = \beta_i$:

$$\begin{aligned} \frac{x_i}{x_0} &= \left(\beta_i - \varepsilon_2^{(\nu)}\right) \kappa_2^{(\nu)} + \left(\beta_i - \varepsilon_1^{(\nu)}\right) \kappa_1^{(\nu)} + \left(\beta_i - \varepsilon_0^{(\nu)}\right) \kappa_0^{(\nu)} \\ &= \beta_i - \left(\varepsilon_2^{(\nu)} \kappa_2^{(\nu)} + \varepsilon_1^{(\nu)} \kappa_1^{(\nu)} + \varepsilon_0^{(\nu)} \kappa_0^{(\nu)}\right) \end{aligned}$$

wo II, 194

$$\lim_{\nu=\infty} \varepsilon_2^{(\nu)}, \varepsilon_1^{(\nu)}, \varepsilon_0^{(\nu)} = 0.$$

Daher folgt für $\nu \geqq \nu_0(\varepsilon)$:

$$\left|\varepsilon_2^{(\nu)} \kappa_2^{(\nu)} + \varepsilon_1^{(\nu)} \kappa_1^{(\nu)} + \varepsilon_0^{(\nu)} \kappa_0^{(\nu)}\right| < \varepsilon \left(\kappa_2^{(\nu)} + \kappa_1^{(\nu)} + \kappa_0^{(\nu)}\right) = \varepsilon$$

also im $\lim\limits_{\nu=\infty} = 0$, daher

$$\frac{x_i}{x_0} = \beta_i = \lim_{\nu=\infty} \frac{\mathsf{A}_i^{(\nu)}}{\mathsf{A}_0^{(\nu)}}\,; \qquad \text{w. z. b. w.}$$

c.) Eindeutigkeitsbeweis.

Der eben geführte Existenzbeweis für den lim der Näherungsbrüche läßt sich so auffassen, daß jedem System von Zahlen $a_1^{(\nu)}, a_2^{(\nu)}$; $(\nu = 0, 1, \dots)$, die den Bedingungen:

$$\text{(I.)} \qquad a_2^{(\nu)} \geqq 1\,; \quad a_2^{(\nu)} \geqq a_1^{(\nu)} \geqq 0\,; \quad (\nu \geqq 1)$$

genügen, ein konvergenter Jacobi–Algorithmus entspricht, der aus den formal abgeleiteten Rekursionsformeln für die $\mathsf{A}_i^{(\nu)}$ besteht.

Liegt nun ein solcher Algorithmus vor, d. h. sind die Zahlen $\mathsf{A}_i^{(\nu)}$ aus den $a_i^{(\nu)}$ berechnet und x_0, x_1, x_2 drei Zahlen, gegen deren Verhältnisse er konvergiert $(x_0 > 0)$, so ist keineswegs selbstverständlich, daß die Jacobi Entwicklung für x_0, x_1, x_2 gerade die Zahlen $a_i^{(\nu)}$ liefert. Es könnten ja mehrere solche formale Entwicklungen gegen die nämliche Grenze konvergieren. Tatsächlich müssten II, 195 auch die $a_i^{(\nu)}$ außer der Konvergenzbedingung (I.) noch einer weiteren Bedingung genügen, damit dies der Fall ist. Die letztere Bedingung folgt aus der Bemerkung, daß die Zahlen $a_i^{(\nu)}$ eines wirklichen Jacobi Algorithmus außer der Bedingung (I.) noch einer weiteren Einschränkung

(II.) *Wenn* $a_2^{(\nu)} = a_1^{(\nu)}$, *so ist* $a_1^{(\nu+1)} \geqq 1$; $(\nu \geqq 1)$

unterworfen sind. Wir beweisen nun:

Satz 2. *Durch die Bedingungen* (I.),(II.) *ist ein Jacobi–Algorithmus eindeutig festgelegt, d. h. die Grenzwerte, gegen die die Verhältnisse der aus den* $a_i^{(\nu)}$ *gebildeten* $\mathsf{A}_i^{(\nu)}$ *konvergieren, liefern, in einen Jacobi Algorithmus entwickelt, genau die Entwicklungszahlen* $a_i^{(\nu)}$. *Anders ausgedrückt:*
Stimmen die Grenzwerte der $\mathsf{A}_i^{(\nu)}$ *und* $\mathsf{B}_i^{(\nu)}$ *von* 2 *Entwicklungsreihen* $a_i^{(\nu)}$ *und* $b_i^{(\nu)}$ *überein, so stimmen auch die* $a_i^{(\nu)}$ *und* $b_i^{(\nu)}$ *überein; Jedes System* x_0, x_1, x_2 *von* 3 *linear unabhängigen Zahlen* $(x_0 > 0)$, *gestattet nur eine einzige Entwicklung, die den Bedingungen* (I.),(II.) *genügt.* (I.),(II.) *sind also die einzigen Einschränkungen, denen die Entwicklungszahlen unterworfen sind.*

Beweis: Wir haben zunächst einiges Formale nachzuholen. Es seien $a_1^{(\nu)}, a_2^{(\nu)}$; $(\nu \geqq 0)$ die Entwicklungszahlen eines Algorithmus, $\mathsf{A}_i^{(\nu)}$ die aus ihnen gebildeten Näherungswerte und x_0, x_1, x_2, $(x_0 > 0)$ ein Tripel von Zahlen, gegen die der den Bedingungen (I.) und (II.) genügende Algorithmus konvergiert. II, 196

Neben den $\mathsf{A}_i^{(\nu)}$ betrachten wir dann die Größen $\mathsf{A}_{i,\kappa}^{(\nu)}$, die aus dem mit $a_1^{(\kappa)}, a_2^{(\kappa)}$ beginnenden Algorithmus definiert sind, wie die $\mathsf{A}_i^{(\nu)}$ aus dem mit $a_1^{(0)}, a_2^{(0)}$ beginnenden, sodaß also

$$\mathsf{A}_{i,0}^{(\nu)} = \mathsf{A}_i^{(\nu)}$$

ist. Für $\kappa \geqq 1$ sind dann die $\mathsf{A}_{i,\kappa}^{(\nu)}$ sämtlich $\geqq 0$, da die $a_i^{(\kappa)}$ für $\kappa \geqq 1$ den Bedingungen (I.) genügen. Es sei $x_0^{(\kappa)}, x_1^{(\kappa)}, x_2^{(\kappa)}$ je ein Wertetripel, gegen das die $\mathsf{A}_{i,\kappa}^{(\nu)}$ konvergieren; diese seien so normiert, daß erstens, wie stets, $x_0^{(\kappa)} > 0$, und zweitens, daß

$$x_2^{(\kappa)} = x_0^{(\kappa-1)}; \quad (\kappa \geqq 1)$$

ist. Wie aus dem Beweis zu Satz 1 zu entnehmen, sind die $x_i^{(\kappa)}$ für $\kappa \geqq 1$ sämtlich > 0.

In den folgenden Matrizen bezeichnet i den Zeilenindex, κ den Spaltenindex, die beide von 2 bis 0 laufen. Ferner sei bezeichnet zur Abkürzung:

$$\mathsf{R}_\nu = \begin{pmatrix} a_2^{(\nu)} & 1 & 0 \\ a_1^{(\nu)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}; \quad (\nu \geqq 0)$$

Dann besteht die Formel: II, 197

$$\left(\mathsf{A}_i^{(\lambda+\nu+\kappa)}\right) = \left(\mathsf{A}_i^{(\lambda+\kappa)}\right) \mathsf{R}_\lambda \mathsf{R}_{\lambda+1} \dots \mathsf{R}_{\lambda+\nu-1}\,; \qquad (\nu \geqq 1;\ \lambda \geqq 0)\,.$$

Ferner gilt die explizite Formel

$$\left(\mathsf{A}_i^{(\nu+\kappa)}\right) = \mathsf{R}_0 \mathsf{R}_1 \dots \mathsf{R}_{\nu-1}\,; \quad (\nu \geqq 1)$$

woraus nach Definition der $\mathsf{A}_{i,\lambda}^{(\nu)}$ folgt:

$$\left(\mathsf{A}_{i,\lambda}^{(\nu+\kappa)}\right) = \mathsf{R}_\lambda \mathsf{R}_{\lambda+1} \dots \mathsf{R}_{\lambda+\nu-1}\,; \quad (\nu \geqq 1;\ \lambda \geqq 0)$$

Zusammengenommen ist also:

$$\left(\mathsf{A}_i^{(\lambda+\nu+\kappa)}\right) = \left(\mathsf{A}_i^{(\lambda+\kappa)}\right)\left(\mathsf{A}_{i,\lambda}^{(\nu+\kappa)}\right); \quad (\nu \geqq 1;\ \lambda \geqq 0)$$

Durch Übergang zu den Elementen folgt hieraus:

$$\mathsf{A}_i^{(\lambda+\nu)} = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(\lambda+\kappa)} \mathsf{A}_{\kappa,\lambda}^{(\nu)}; \quad (\nu \geqq 1;\ \lambda \geqq 0).$$

Speziell ist also für $\lambda = 1$:

$$\mathsf{A}_i^{(\nu+1)} = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(\kappa+1)} \mathsf{A}_{\kappa,1}^{(\nu)}; \quad (\nu \geqq 1).$$

Aus

$$\left(\mathsf{A}_i^{(\kappa+1)}\right) = \begin{pmatrix} a_2^{(0)} & 1 & 0 \\ a_1^{(0)} & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

folgt also:

$$\begin{aligned} \mathsf{A}_2^{(\nu+1)} &= \mathsf{A}_{2,1}^{(\nu)} a_2^{(0)} + \mathsf{A}_{1,1}^{(\nu)} \\ \mathsf{A}_1^{(\nu+1)} &= \mathsf{A}_{2,1}^{(\nu)} a_1^{(0)} + \mathsf{A}_{0,1}^{(\nu)} \\ \mathsf{A}_0^{(\nu+1)} &= \mathsf{A}_{2,1}^{(\nu)} \end{aligned}$$

II, 198 oder durch Grenzübergang zu $\nu = \infty$ unter Berücksichtigung von $x_2^{(1)} = x_0$:

$$x_2 = a_2^{(0)} x_0 + x_1^{(1)}; \quad x_1 = a_1^{(0)} x_0 + x_0^{(1)}$$

Benutzt man ferner die obigen Formeln, angewendet auf den mit $a_1^{(\kappa)}, a_2^{(\kappa)}$ beginnenden Algorithmus, zu dem $a_1^{(\kappa+1)}, a_2^{(\kappa+2)}$ in derselben Beziehung steht, wie $a_1^{(1)}, a_2^{(1)}$ zu dem mit $a_1^{(0)}, a_2^{(0)}$ beginnenden, so folgt genau so, unter Berücksichtigung von $x_2^{(\kappa+1)} = x_0^{(\kappa)}$:

$$x_2^{(\kappa)} = a_2^{(\kappa)} x_0^{(\kappa)} + x_1^{(\kappa+1)}; \quad x_1^{(\kappa)} = a_1^{(\kappa)} x_0^{(\kappa)} + x_0^{(\kappa+1)}; \quad (\kappa \geqq 0).$$

Da die $x_i^{(\kappa+1)}$ und $x_0^{(\kappa)}$ für $\kappa \geqq 0$ positiv sind, folgt

$$\frac{x_2^{(\kappa)}}{x_0^{(\kappa)}} > a_2^{(\kappa)}; \quad \frac{x_1^{(\kappa)}}{x_0^{(\kappa)}} > a_1^{(\kappa)}; \quad (\kappa \geqq 0).$$

Wir benutzen nun die Voraussetzungen (I.),(II.) über die $a_i^{(\kappa)}$. Nach (I.) ist $a_2^{(\kappa)} \leqq 1$ für $\kappa \geqq 1$, daher auch $x_2^{(\kappa)} > x_0^{(\kappa)}$ für $\kappa \geqq 1$. Somit ist wegen $x_0^{(\kappa-1)} = x_2^{(\kappa)}$ und

$$x_1^{(\kappa-1)} = a_1^{(\kappa-1)} x_0^{(\kappa-1)} + x_0^{(\kappa)}$$

sicher

$$x_1^{(\kappa-1)} - \left(a_1^{(\kappa-1)} + 1\right) x_0^{(\kappa-1)} = x_0^{(\kappa)} - x_0^{(\kappa-1)} = x_0^{(\kappa)} - x_2^{(\kappa)} < 0; \quad (k \geqq 1)$$

und daher zusammengenommen

$$a_1^{(\kappa)} < \frac{x_1^{(\kappa)}}{x_0^{(\kappa)}} < a_1^{(\kappa)} + 1; \quad (\kappa \geqq 0),$$

d. h. stets $a_1^{(\kappa)}$ das größte Ganze in $\frac{x_1(\kappa)}{x_0^{(\kappa)}}$. Ferner ist nach (I.) für $\kappa \geqq 1$: $a_2^{(\kappa)} \geqq$ II, 199 $a_1^{(\kappa)}$. Falls nun $a_2^{(\kappa)} > a_1^{(\kappa)}$, so folgt

$$\frac{x_2^{(\kappa)}}{x_0^{(\kappa)}} > a_2^{(\kappa)} \geqq a_1^{(\kappa)} + 1 > \frac{x_1^{(\kappa)}}{x_0^{(\kappa)}}; \quad (\kappa \geqq 1)$$

also

$$x_2^{(\kappa)} > x_1^{(\kappa)}; \quad (\kappa \geqq 1)$$

Falls aber $a_2^{(\kappa)} = a_1^{(\kappa)}$, so ist nach (II.) $a_1^{(\kappa+1)} \geqq 1$, daher

$$\frac{x_2^{(\kappa)}}{x_0^{(\kappa)}} = a_2^{(\kappa)} + \frac{x_1^{(\kappa+1)}}{x_0^{(\kappa)}} > a_1^{(\kappa)} + a_1^{(\kappa+1)} \frac{x_0^{(\kappa+1)}}{x_0^{(\kappa)}} \geqq a_1^{(\kappa)} + \frac{x_0^{(\kappa+1)}}{x_0^{(\kappa)}}$$
$$= \frac{x_1^{(\kappa)}}{x_0^{(\kappa)}}; \quad (\kappa \geqq 1),$$

also auch hier

$$x_2^{(\kappa)} > x_1^{(\kappa)}; \quad (\kappa \geqq 1).$$

Somit ist

$$\frac{x_2^{(\kappa-1)}}{x_0^{(\kappa-1)}} = a_2^{(\kappa-1)} + \frac{x_1^{(\kappa)}}{x_0^{(\kappa-1)}} = a_2^{(\kappa-1)} + \frac{x_1^{(\kappa)}}{x_2^{(\kappa)}} < a_2^{(\kappa-1)} + 1; \qquad (\kappa \geqq 1)$$

und somit zusammengenommen:

$$a_2^{(\kappa)} < \frac{x_2^{(\kappa)}}{x_0^{(\kappa)}} < a_2^{(\kappa)} + 1; \quad (\kappa \geqq 0)$$

Es ist also auch stets $a_2^{(\kappa)}$ das größte Ganze in $\frac{x_2^{(\kappa)}}{x_0^{(\kappa)}}$. Damit ist die formale Identität mit dem Jacobi Algorithmus von x_0, x_1, x_2 nachgewiesen, und Satz 2 bewiesen.

II, 200

d.) Periodische Algorithmen.

Ein Jacobi–Algorithmus heißt periodisch, wenn die $a_i^{(\nu)}$ von einem $\nu = \lambda$ an sich mit einer Periode von einer Länge $n \geqq 1$ wiederholen. Das kleinste n dieser Art heißt die *Zeilenzahl der Periode*, das kleinste λ die *Zeilenzahl der Vorperiode.* Für $\lambda = 0$ heißt die Entwicklung *reinperiodisch*, für $\lambda > 0$ *gemischt periodisch.* Wir betrachten zunächst die $a_i^{(\nu)}$ als unbestimmte Variable. Bezeichnen wieder i und κ die von 2 bis 0 laufenden Zeilen– und Spalten–Indizes, so heißt die Gleichung

$$\left| \left(\mathsf{A}_i^{(\lambda+n+\kappa)} \right) - \varrho \left(\mathsf{A}_i^{(\lambda+\kappa)} \right) \right| = 0, \tag{1}$$

für einen Algorithmus mit n zeiliger Periode und λ–zeiliger Vorperiode die *charakteristische Gleichung* des Algorithmus.

Satz 3. *Die charakteristische Gleichung hängt nur von den Entwicklungszahlen $a_i^{(\lambda)}, \dots a_i^{(\lambda+n-1)}$ der reinen Periode ab. Sie läßt sich nämlich auch in der Form schreiben:*

$$\left| \left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} \right) - \varrho \mathsf{E} \right| = 0. \tag{2}$$

Beweis: Nach S. 197] gilt

$$\left(\mathsf{A}_i^{(\lambda+n+\kappa)} \right) = \left(\mathsf{A}_i^{(\lambda+\kappa)} \right) \left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} \right) \quad \text{für } n \geqq 1;\ \lambda \geqq 0.$$

Multipliziert man also (2) mit $\left|\mathsf{A}_i^{(\lambda+\kappa)}\right| \neq 0$, so entsteht wegen II, 201

$$\left(\mathsf{A}_i^{(\lambda+\kappa)}\right)\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} - \varrho\mathsf{E}\right) = \left(\mathsf{A}_i^{(\lambda+\kappa)}\right)\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)}\right) - \varrho\left(\mathsf{A}_i^{(\lambda+\kappa)}\right)$$

durch Determinantenbildung gerade (1).

Satz 4. *Sind $\varrho_0, \varrho_1, \varrho_2$ die 3 Wurzeln der charakteristischen Gleichung, so genügen $\varrho_0^\nu, \varrho_1^\nu, \varrho_2^\nu$ der Gleichung*

$$\left|\left(\mathsf{A}_{i,\lambda}^{(n\nu+\kappa)}\right) - x\mathsf{E}\right| = 0\,; \quad (\nu \geqq 1). \tag{3}$$

Die Gleichungen (3), speziell also auch (1),(2) sind irreduzibel im Bereich der rationalen Funktionen der $a_i^{(\nu)}$.

Beweis: 1.) Sei ϱ Wurzel von (2) und ζ eine primitive ν–te Einheitswurzel. Dann bilden wir

$$\prod_{r=0}^{\nu-1}\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} - \varrho\zeta^r\mathsf{E}\right).$$

Wegen elementarer Eigenschaften der ζ^r ist dies

$$= \left(\mathsf{A}_{i,\lambda}^{(n+\kappa)}\right)^\nu - \varrho^\nu\mathsf{E}.$$

Nun ist aber nach S. 197]

$$\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)}\right) = \mathsf{R}_\lambda\mathsf{R}_{\lambda+1}\ldots\,\mathsf{R}_{\lambda+\nu-1}\,,$$

und da sich die R_ν periodisch wiederholen, d. h.

$$\mathsf{R}_{\lambda+n} = \mathsf{R}_\lambda\,,\ldots$$

ist, folgt:

$$\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)}\right)^\nu = \left(\mathsf{A}_{i,\lambda}^{(n\nu+\kappa)}\right).$$

Daher folgt: II, 202

$$\prod_{r=0}^{\nu-1}\left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} - \varrho\zeta^r\mathsf{E}\right) = \left(\mathsf{A}_{i,\lambda}^{(n\nu+\kappa)}\right) - \varrho^\nu\mathsf{E},$$

also durch Determinantenbildung, weil links der erste Faktor nach (2) Null ist,

$$\left|\mathsf{A}_{i,\lambda}^{(n\nu+\kappa)} - \varrho^\nu\mathsf{E}\right| = 0,$$

d. h. ϱ^ν ist Wurzel von (3).

2.) Zum Nachweis der Irreduzibilität von (3) für unbestimmte $a_i^{(\nu)}$ setzen wir speziell $a_i^{(\nu)}$ unabhängig von ν gleich a_i und zeigen die Irreduzibilität in diesem Spezialfall, dann folgt sie auch allgemein. Formal bedeutet dies, daß wir einen einzeilig periodischen Algorithmus betrachten, d. h. einfach $n = 1$ annehmen. Dann wird (3) zunächst für $\nu = 1$ $\big($also (2)$\big)$ zu

$$\begin{aligned} \left|\mathsf{A}_{i,\lambda}^{(\kappa+1)} - x\mathsf{E}\right| &= |\mathsf{R}_\lambda - x\mathsf{E}| \\ &= \begin{vmatrix} a_2 - x & 1 & 0 \\ a_1 & -x & 1 \\ 1 & 0 & -x \end{vmatrix} \\ &= x^2(a_2 - x) + 1 + a_1 x = -x^3 + a_2 x + a_1 x + 1 \end{aligned} \tag{4}$$

Diese Gleichung ist aber irreduzibel für unbestimmte a_1, a_2. Die Gleichung (3) ist dann aufzufassen als Gleichung, der die $n\nu$–ten Potenzen der Wurzeln von (4) genügen. Wäre also (3) reduzibel, so wäre die $n\nu$–te Potenz einer Wurzel von (4) rational durch a_1, a_2 darstellbar, also (4) durch Ausziehung einer $n\nu$–ten Wurzel lösbar, während doch (4) für spezielle a_1, a_2 sicher (auch nach Adjunktion von Einheitswurzeln zum Grundkörper) *nicht–zyklisch* gemacht werden kann. Also muß (3) irreduzibel sein für den Fall $a_i^{(\lambda)} = a_i^{(\lambda+1)} = \cdots = a_i$, umsomehr für beliebige $a_i^{(\nu)}$. Damit ist Satz 4 bewiesen.

II, 203

Satz 5. *Die charakteristische Gleichung* (2) *ändert sich nicht, wenn die* $a_i^{(\nu)}$ *innerhalb der Periode zyklisch permutiert werden.*

Beweis: Es ist die Identität von (2) mit

$$\left|\mathsf{A}_{i,\lambda+1}^{(n+\kappa)} - \varrho\mathsf{E}\right| = 0$$

nachzuweisen. Nun ist aber

$$\left(\mathsf{A}_{i,\lambda+1}^{(n+\kappa)}\right) = \mathsf{R}_{\lambda+1} \dots \mathsf{R}_{\lambda+n} = \mathsf{R}_\lambda^{-1} \left(\mathsf{A}_{i,\lambda}^{(n+\kappa)}\right) \mathsf{R}_{\lambda+n} .$$

Also folgt

$$\mathsf{R}_\lambda^{-1} \left(\mathsf{A}_{i,\lambda}^{(n+\kappa)} - \varrho\mathsf{E}\right) \mathsf{R}_{\lambda+n} = \left(\mathsf{A}_{i,\lambda+1}^{(n+\kappa)} - \varrho\mathsf{E}\mathsf{R}_\lambda^{-1}\mathsf{R}_{\lambda+n}\right)$$

und wegen $\mathsf{R}_\lambda = \mathsf{R}_{\lambda+n}$ die Identität, die wir nachweisen wollten.

Wir nehmen nunmehr an, x_0, x_1, x_2 seien drei linear unabhängige Zahlen eines kubischen reellen Zahlkörpers K. Die Erfahrung bestätigt, daß der zugehörige Jacobi–Algorithmus stets periodisch ist. Wie nehmen demgemäß an, der Algorithmus sei n–zeilig periodisch und λ die Zeilenzahl der Vorperiode. Da dann der Algorithmus für $x_0^{(\lambda)}, x_1^{(\lambda)}, x_2^{(\lambda)}$ reinperiodisch ist, und $x_0^{(\lambda)}, \ldots, x_2^{(\lambda)}$ zu $x_0, \ldots, x_2$ äquivalent, also ebenfalls ein System von 3 linear unabhängigen Zahlen aus K ist, können wir von vornherein annehmen, daß $\lambda = 0$ sei. Dann bestehen die Gleichungen: II, 204

$$(x_i) = \left(\mathsf{A}_i^{(n+\kappa)}\right)\left(x_\kappa^{(n)}\right)$$

und

$$\begin{aligned} x_2 : x_1 : x_0 &= \lim_{\nu=\infty} \mathsf{A}_2^{(\nu)} : \mathsf{A}_1^{(\nu)} : \mathsf{A}_0^{(\nu)} \\ &= \lim_{\nu=\infty} \mathsf{A}_{2,n}^{(\nu+n)} : \mathsf{A}_{1,n}^{(\nu+n)} : \mathsf{A}_{0,n}^{(\nu+n)} = x_2^{(n)} : x_1^{(n)} : x_0^{(n)} \end{aligned}$$

d. h.

$$(x_i) = \varrho'\left(x_i^{(n)}\right) = \varrho'\mathsf{E}\cdot\left(x_\kappa^{(n)})\right)$$

Durch Verbindung folgt:

$$\left(\left(\mathsf{A}_i^{(n+\kappa)}\right) - \varrho'\mathsf{E}\right)\left(x_\kappa^{(n)}\right) = 0,$$

also wegen der linearen Unabhängigkeit der $x_\kappa^{(n)}$ auch

$$\left|\mathsf{A}_i^{(n+\kappa)} - \varrho'\mathsf{E}\right| = 0,$$

d. h. ϱ' ist Wurzel der charakteristischen Gleichung unseres periodischen Algorithmus.

Andererseits ist ϱ' eine Größe aus K als Quotient $\frac{x_0}{x_0^{(n)}} = \frac{x_1}{x_1^{(n)}} = \frac{x_2}{x_2^{(n)}}$. Durch die charakteristische Gleichung wird also eine bestimmte Größe ϱ' des Zahlkörpers K geliefert. Wegen $\left|\mathsf{A}_i^{(n+\kappa)}\right| = 1$ ist offenbar ϱ' eine Einheit aus K. II, 205

Satz 6. *Ist x_0, x_1, x_2 ein System von 3 linear unabhängigen Zahlen eines reell–kubischen Körpers K und sein Jacobi–Algorithmus periodisch, so liefert die charakteristische Gleichung des Algorithmus eine Einheit von K.*

Wir bezeichnen fortan die auf den höchsten Koeffizienten $+1$ normierte charakteristische Gleichung $\left|\varrho\mathsf{E} - \mathsf{A}_i^{(n+\kappa)}\right| = 0$ mit $f(\varrho)$, ihre 2reihigen Unterdeterminanten (Vorzeichen!) mit $g_{i,\kappa}(\varrho)$. Die $g_{i,\kappa}(\varrho)$ sind ganzzahlige Polynome in ϱ. Da $f(\varrho') = 0$, hat das Gleichungssystem

$$\varrho' x_i = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(\nu+\kappa)} x_\kappa$$

die Lösung:

$$x_2 : x_1 : x_0 = g_{2,\kappa}(\varrho') : g_{1,\kappa}(\varrho') : g_{0,\kappa}(\varrho')$$

($\kappa = 0, 1$ oder 2). Wir werden später zeigen, daß die $g_{i,\kappa}(\varrho')$ für das hier zu wählende ϱ' stets positiv sind, jedenfalls also nicht alle verschieden. Daraus folgt, II, 206 daß auch $g_{2,\kappa}(\varrho'), g_{1,\kappa}(\varrho'), g_{0,\kappa}(\varrho')$ linear unabhängig, und daher ϱ' primitives Element ist, d. h. $f(\varrho)$ irreduzibel.

Satz 7. *Die charakteristische Gleichung eines aus drei linear unabhängigen Zahlen eines reellen kubischen Körpers K entspringenden, periodischen Jacobi Algorithmus ist irreduzibel, die durch sie gelieferte Einheit ϱ' von K also verschieden von ± 1 (und Einheitswurzeln).*

e.) Eigenschaften der charakteristischen Gleichung.

Wir beweisen zunächst folgenden Hilfssatz über charakteristische Gleichungen total positiver Matrizen:

Satz 8. *Ist A eine Matrix mit positiven Koeffizienten, so hat die charakteristische Gleichung*

$$f(\varrho) = |\varrho\mathsf{E} - \mathsf{A}| = 0$$

mindestens eine positive Wurzel; ihre größte positive Wurzel ϱ_0 ist einfach und ihre „ersten“ Unterdeterminanten sind für $\varrho = \varrho_0$ positiv.

Beweis: Da der Satz für einreihige Matrizen evident ist, sei er für n reihige bewiesen und

$$\mathsf{A} = (a_{i\kappa}) \ ; \quad (i, \kappa = 0, 1, \ldots n)$$

$(n+1)$–reihig. Es sei $\mathsf{A}_0 = (a_{i\kappa})$; $(i, \kappa = 1, \ldots n)$ und

$$f_0(\varrho) = |\varrho\mathsf{E} - \mathsf{A}_0|$$

II, 207 Für $f_0(\varrho)$ gilt dann der Satz. Es sei ϱ' die größte positive Wurzel von $f_0(\varrho)$.

Das Gleichungssystem

$$\sum_{i=1}^{n} a_{i\kappa}\eta_i = \varrho'\eta_\kappa$$

hat dann die Determinante $f_0(\varrho') = 0$, sodaß eine von Null verschiedene Lösung existiert:

$\eta_1 : \eta_2 : \ldots : \eta_\kappa =$ Verhältnis der $(n-1)$ reihigen Unterdeterminanten irgendeiner Spalte von $f_0(\varrho')$.

Das ist n. V. ein Verhältnis positiver Zahlen.

Wir definieren weiter $\xi_1(\varrho), \ldots, \xi_n(\varrho)$ durch

$$a_{i0} + \sum_{\kappa=1}^{n} a_{i\kappa}\xi_\kappa(\varrho) = \varrho\xi_i(\varrho)\,; \quad i = 1, 2, \ldots n.$$

Die Determinante ist $|\varrho\mathsf{E} - \mathsf{A}_0| = f_0(\varrho)$. Die ξ_i sind daher rationale Funktionen von ϱ mit dem Nenner $f_0(\varrho)$. Bildet man

$$(\varrho - a_{00}) - a_{01}\xi_1 - \cdots - a_{0n}\xi_n\,,$$

so entsteht durch Erweiterung mit $f_0(\varrho)$ gerade die Entwicklung von $f(\varrho)$ nach der ersten Zeile, also

$$\varrho - a_{00} - a_{01}\xi_1 - \cdots - a_{0n}\xi_n = \frac{f(\varrho)}{f_0(\varrho)}\,.$$

Für $\varrho > \varrho'$ ist nach Annahme $f_0(\varrho) \neq 0$, also > 0, da der höchste Koeffizient $+1$. Die ξ_i können also, da sie für $\varrho > \varrho'$ stetige Funktionen von ϱ sind, dort ihr Zeichen nur beim Durchgang durch Null wechseln. II, 208

Nun sind die ξ_i im Unendlichen 0, da ihre Zähler in ϱ von niederem Grade sind, als der Nenner $f_0(\varrho)$. Daher gelten folgende, aus dem Definitionsgleichungssystem sofort zu entnehmende Laurent–Reihen:

$$\xi_i = \frac{a_{i0}}{\varrho} + \cdots$$

Daher sind die ξ_i für große ϱ sämtlich positiv und beliebig klein und daher auch für große ϱ

$$\frac{f(\varrho)}{f_0(\varrho)} > 0.$$

Geht $\varrho \to \varrho'$, so müssen die ξ_i positiv bleiben. Denn ginge zuerst ξ_i durch Null, so folgte für das betr. ϱ aus

$$\xi_i = a_{i0} + \sum_{\kappa=1}^{n} a_{i\kappa}\xi_\kappa \geqq a_{i0} > 0$$

ein Widerspruch.

Für $\varrho = \varrho'$ dagegen ist sicher ein $\xi_i = \infty$. Denn sonst wären alle Determinanten aus den letzten n Zeilen von $f(\varrho)$ gleich Null, also die Spalte (a_{i0}) abhängig von den n Spalten $(a_{i1}), (a_{i2}), \dots (a_{in})$ mit $-\varrho$ an der Diagonalstelle, d. h. die obigen Größen η_i befriedigten auch die Gleichung

$$\sum_{i=1}^{n} a_{i0}\eta_i = 0$$

was nur für $\eta_i = 0$ möglich.

Damit folgt aus $\varrho - a_{00} - \sum_{\kappa=1}^{n} a_{0\kappa}\xi_\kappa = \frac{f(\varrho)}{f'(\varrho)}$ für $\varrho \to \varrho'$ daß $\frac{f(\varrho)}{f'(\varrho)}$ negativ wird, und somit ein größtes $\varrho_0 > \varrho'$ existiert, für das $f(\varrho_0) = 0$, $f_0(\varrho_0) \neq 0$ ist. Da ferner $f_0(\varrho), \xi_1(\varrho), \dots, \xi_n(\varrho) > 0$ für $\varrho > \varrho_0$, so sind auch die Unterdeterminanten der 1. Zeile: $f_0(\varrho)$ und $f_0(\varrho)\xi_i(\varrho)$ sämtlich > 0 für $\varrho > \varrho_0$. Da die 1. Zeile von $f(\varrho)$ von den anderen nicht bevorzugt ist, gilt dies allgemein.

II, 209

Schließlich muß ϱ_0 einfach sein. Denn es ist

$$\varrho\frac{d\xi_i}{d\varrho} = -\xi_i + \sum_{\kappa=1}^{n} a_{i\kappa}\frac{d\xi_n}{d\varrho}\,.$$

Für große ϱ ist $\frac{d\xi_i}{d\varrho} = -\frac{a_{i0}}{\varrho^2} + -$ negativ. Für $\varrho \to \varrho'$ müssen diese Größen negativ bleiben, da für das erste $\frac{d\xi_i}{d\varrho} = 0$ folgte

$$0 = \varrho\frac{d\xi_i}{d\varrho} \leqq -\xi_i < 0.$$

Daher ist

$$\frac{d}{d\varrho}\left(\frac{f(\varrho)}{f_0(\varrho)}\right)_{\varrho=\varrho_0} > 0\,, \quad \text{also } f'(\varrho_0) > 0,$$

w. z. b. w.

In einem Jacobi–Algorithmus ist von einem gewissen ν an sicher $\mathsf{A}_i(\nu) > 0$. Daher genügt für hinreichend hohe ν die Gleichung

$$f_\nu(\sigma) = \left|\sigma\mathsf{E} - \mathsf{A}_i^{(\nu n+\kappa)}\right| = 0$$

den Voraussetzungen von Satz 8. Es sei σ_0 ihre größte positive Wurzel, die einfach ist, und $g_{i,\kappa}^{(\nu)}(\sigma)$ ihre ersten Unterdeterminanten, sodaß $g_{i,\kappa}^{(\nu)}(\sigma_0) > 0$ ist. II, 210

Nach Satz 4 ist $f_\nu(\sigma)$ die Gleichung, der die ν–ten Potenzen der Wurzeln der charakteristischen Gleichung $f(\sigma) = f_1(\sigma)$ genügen, also $\sigma_0 = \varrho_0^\nu$ die ν–te Potenz einer Wurzel von $f(\varrho)$. Wäre ϱ_0 nicht positiv, so müßte $\frac{\varrho_0}{|\varrho_0|}$ eine ν–te Einheitswurzel sein. Da ν beliebig viele beliebig große Werte annehmen kann, und also mindestens eine der drei Wurzeln von $f(\varrho)$ so unendlich oft betroffen ist, müßte dies $\frac{\varrho_0}{|\varrho_0|}$ Einheitswurzel beliebig hohen Grades, also 1 sein. Eine kleinere positive Wurzel von $f(\varrho)$ kann nicht existieren, da dann auch $f_\nu(\sigma)$ eine solche hätte. Also hat auch $f(\varrho)$ eine größte positive Wurzel, und diese ist einfach, weil es $\sigma_0 = \varrho_0^\nu$ ist.

Weiter beweisen wir, daß auch die Unterdeterminanten $g_{i,\kappa}(\varrho_0) > 0$ sind. Es ist nämlich

$$\begin{aligned} f_\nu(\sigma) &= (\sigma - \varrho_0^\nu)(\sigma - \varrho_1^\nu)(\sigma - \varrho_2^\nu) \\ f_\nu(\varrho^\nu) &= (\varrho^\nu - \varrho_0^\nu)(\varrho^\nu - \varrho_1^\nu)(\varrho^\nu - \varrho_2^\nu) \\ &= (-1)^{\nu+1} \prod_{\kappa=0}^{2} \prod_{r=0}^{\nu-1} (\varepsilon^r \varrho - \varrho_\kappa) = (-1)^{\nu+1} \prod_{r=0}^{\nu-1} f(\varepsilon^r \varrho) \end{aligned}$$

wo ε eine primitive ν–te Einheitswurzel ist. Für $\varrho = \varrho_0$ verschwindet der Faktor $f(\varrho_0)$ aber kein weiterer, da sonst $\varepsilon^r \varrho_0 - \varrho_\kappa = 0$, also $\kappa \neq 0$ und $\varrho_0^\nu = \varrho_\kappa^\nu$ wäre, während doch $\varrho_0^\nu = \sigma_0$ einfache Wurzel von $f_\nu(\sigma)$ ist. II, 211

Nun sind die $g_{i,\kappa}^{(\nu)}(\sigma)$ offenbar Polynome 2. Grades in σ, während $f_\nu(\sigma)$ den Grad 3 hat, also gestatten die Funktionen $\frac{g_{i,\kappa}^{(\nu)}(\sigma)}{f_\nu(\sigma)}$ eine Entwicklung nach negativen Potenzen von $\frac{1}{\sigma}$, die mit der Potenz $\frac{1}{\sigma}$ beginnt.

Ich behaupte, daß

$$\frac{g_{i,\kappa}^{(\nu)}(\sigma)}{f_\nu(\sigma)} = \sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\sigma^{\mu+1}}$$

ist. In der Tat ist die Matrix $\left(\frac{g_{i,\kappa}^{(\nu)}(\sigma)}{f_\nu(\sigma)}\right)$ eindeutig als reziproke zu $\left(\sigma\mathsf{E} - \mathsf{A}_i^{(\nu n+\kappa)}\right)$ bestimmt. Es ist also nur zu zeigen, daß die obigen Laurent–Reihen der Relation genügen:

$$\left(\sigma\mathsf{E} - \mathsf{A}_i^{(\nu n+\kappa)}\right)\left(\sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\sigma^{\mu+1}}\right) = \mathsf{E}$$

II, 212 Nun ist

$$\left(\sigma \mathsf{E} - \mathsf{A}_i^{(\nu n+\kappa)}\right)\left(\sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\sigma^{\mu+1}}\right) = \left(\sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{\mu\nu n+\kappa}}{\sigma^{\mu}}\right) - \sum_{\mu=0}^{\infty} \frac{1}{\sigma^{\mu+1}} \left(\mathsf{A}_i^{(\nu n+\kappa)}\right)\left(\mathsf{A}_i^{(\mu n+\kappa)}\right)$$

$$= \sum_{\mu=0}^{\infty} \frac{\left(\mathsf{A}_i^{\mu\nu n+\kappa}\right)}{\sigma^{\mu}} - \sum_{\mu=0}^{\infty} \frac{\left(\mathsf{A}_i^{((\mu+1)\nu n+\kappa)}\right)}{\sigma^{\mu+1}} = \left(\mathsf{A}_i^{(\kappa)}\right) = \mathsf{E}.$$

Satz 9. *Die reziproke Matrix zu* $\left(\sigma \mathsf{E} - \mathsf{A}_i^{(\nu n+\kappa)}\right)$ *ist die Matrix*

$$\left(\frac{g_{i,\kappa}^{(\nu)}(\sigma)}{f_\nu(\sigma)}\right) = \left(\sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\sigma^{\mu+1}}\right).$$

Hieraus folgt nun weiter:

$$\frac{g_{i,\kappa}^{(\nu)}(\varrho^\nu)}{f_\nu(\varrho^\nu)} = \sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\varrho^{\nu\mu+\nu}}.$$

Andererseits folgt für $\nu = 1$:

$$\frac{g_{i,\kappa}(\varrho)}{f(\varrho)} = \sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu+\kappa)}}{\varrho^{\mu+1}}$$

und

$$\frac{g_{i,\kappa}(\varepsilon^r \varrho)}{f(\varepsilon^r \varrho)} = \sum_{\mu=0}^{\infty} \frac{1}{\varepsilon^{r(\mu+1)}} \frac{\mathsf{A}_i^{(\mu n+\kappa)}}{\varrho^{\mu+1}}$$

also

$$\sum_{r=0}^{\nu-1} \varepsilon^r \frac{g_{i,\kappa}(\varepsilon^r \varrho)}{f(\varepsilon^r \varrho)} = \sum_{\mu=0}^{\infty}\sum_{r=0}^{\nu-1} \varepsilon^{-\mu r} \frac{\mathsf{A}_i^{(\mu n+\kappa)}}{\varrho^{\mu+1}} = \nu \sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu\nu n+\kappa)}}{\varrho^{\mu\nu+1}}$$

$$= \nu \varrho^{\nu-1} \frac{g_{i,\kappa}^{(\nu)}(\varrho^\nu)}{f_\nu(\varrho^\nu)}$$

Daher folgt für $\varrho = \varrho_0$ wegen $f(\varepsilon^r \varrho_\nu) \neq 0$ für $r > 0$, nach Multiplikation mit $f(\varrho)$: II, 213

$$g_{i,\kappa}(\varrho_0) = \nu \varrho_0^{\nu-1} \frac{g_{i,\kappa}^{(\nu)}(\sigma_0)}{(-1)^{\nu+1} \prod_{r=1}^{\nu} f(\varepsilon^r \varrho_0)}$$

Für ungerades ν ist der Nenner positiv (je 2 Faktoren konjugiert komplex!), also wegen $g_{i,\kappa}^{(\nu)}(\sigma_0) > 0$ auch $g_{i,\kappa}(\varrho_0) > 0$.

Satz 10. *Die Unterdeterminanten $g_{i,\kappa}(\varrho)$ von $\left(\varrho \mathsf{E} - \mathsf{A}_i^{(n+\kappa)}\right)$ sind für die stets vorhandene, größte positive Wurzel ϱ_0 von $f(\varrho) = \left|\varrho \mathsf{E} - \mathsf{A}_i^{(n+\kappa)}\right| = 0$ sämtlich positiv.*

Zusammenfassend haben wir also.

Satz 11. *Sind x_0, x_1, x_2 drei linear unabhängige Zahlen eines reellen kubischen Körpers K, und liefert der Jacobi Algorithmus für sie eine rein–periodische n–zeilige Entwicklung, so liefert die charakteristische Gleichung*

$$f(\varrho) = \left|\varrho \mathsf{E} - \mathsf{A}_i^{(n+\kappa)}\right| = 0$$

des Algorithmus eine größte positive Wurzel ϱ_0. Die 2 reihigen Unterdeterminanten von $f(\varrho)$ sind für ϱ_0 sämtlich positiv.

II, 214

Unser Ziel ist nunmehr nachzuweisen, daß dies bestimmte ϱ_0 mit dem obigen ϱ' identisch, also primitive Größe und Einheit in K ist, für die dann die Gleichungen bestehen

$$\varrho_0 x_i = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(n+\kappa)} x_\kappa\,; \quad (i = 0, 1, 2)$$

und

$$x_2 : x_1 : x_0 = g_{2,\kappa}(\varrho_0) : g_{1,\kappa}(\varrho_0) : g_{0,\kappa}(\varrho_0)\,; \qquad (\kappa = 0, 1, 2).$$

Hierzu gehen wir aus von der Definition von ϱ' vermöge

$$\varrho' x_i = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(n+\kappa)} x_\kappa$$

für einen periodischen Jacobi–Algorithmus von drei linear unabhängigen Zahlen eines reell–kubischen Körpers K. Es ist dann für zwei beliebige Indizes i, λ:

$$\sum_{j=0}^{2}\left(\frac{\mathsf{A}_j^{(\nu n+\lambda)}}{\mathsf{A}_i^{(\nu n+\lambda)}}-\frac{x_j}{x_i'}\right)\mathsf{A}_i^{(n+j)}=\frac{\mathsf{A}_i^{((\nu+1)n+\lambda)}}{\mathsf{A}_i^{(\nu n+\lambda)}}-\frac{1}{x_i}\sum_{j=0}^{2}\mathsf{A}_i^{(n+j)}x_j$$
$$=\frac{\mathsf{A}_i^{((\nu+1)n+\lambda)}}{\mathsf{A}_i^{(\nu n+\lambda)}}-\varrho'.$$

Für $\nu\to\infty$ geht die linke Seite gegen Null, sodaß folgt:

$$\varrho'=\lim_{\nu=\infty}\frac{\mathsf{A}_i^{((\nu+1)n+\lambda)}}{\mathsf{A}_i^{(\nu n+\lambda)}};\quad(\lambda\geqq 0)$$

II, 215 Hieraus folgt weiter:

$$\lim_{\nu=\infty}\frac{\sum_{i=0}^{2}\mathsf{A}_i^{((\nu+1)n+i)}}{\sum_{i=0}^{2}\mathsf{A}_i^{(\nu n+i)}}=\lim_{\nu=\infty}\sum_{i=0}^{2}\frac{\mathsf{A}_i^{((\nu+1)n+i)}}{\mathsf{A}_i^{(\nu n+i)}}\cdot\frac{\mathsf{A}_i^{(\nu n+i)}}{\sum_{j=0}^{2}\mathsf{A}_j^{(\nu n+j)}}$$
$$=\lim_{\nu=\infty}\sum_{i=0}^{2}\frac{\mathsf{A}_i^{((\nu+1)n+i)}}{\mathsf{A}_i^{(\nu n+i)}}\cdot\lambda_i^{(\nu)},\quad\text{wo}\quad\sum_{i=0}^{2}\lambda_i^{(\nu)}=1\quad\text{und}\quad\lambda_i^{(\nu)}\geqq 0$$

ist, also weiter

$$=\lim_{\nu=\infty}\sum_{i=0}^{2}\left(\varrho'-\varepsilon_i^{(\nu)}\right)\lambda_i^{(\nu)}=\varrho'-\lim_{\nu=\infty}\sum_{i=0}^{2}\varepsilon_i^{(\nu)}\lambda_i^{(\nu)},$$

wo die $\varepsilon_i^{(\nu)}$ für $\nu\to\infty$ gegen Null gehen und die $\lambda_i^{(\nu)}$ beschränkt sind. Somit ist also auch

$$\lim_{\nu=0}\frac{\sum_{i=0}^{2}\mathsf{A}_i^{((\nu+1)n+i)}}{\sum_{i=0}^{2}\mathsf{A}_i^{(\nu n+i)}}=\varrho'.$$

Nun genügen die ν–ten Potenzen der Wurzeln ϱ der charakteristischen Gleichung der Gleichung

$$\left|\sigma\mathsf{E}-\mathsf{A}_i^{(\nu n+\kappa)}\right|=0.$$

Daraus folgt, daß die ν–te Potenzsumme der ϱ

$$\sum\varrho^{\nu}=\sum_{i=0}^{2}\mathsf{A}_i^{(\nu n+i)}$$

ist. Also folgt:

$$\varrho' = \lim_{\nu=\infty} \frac{\sum \varrho^{\nu+1}}{\sum \varrho^{\nu}}$$

Es sei nun ϱ_1 der größte der absoluten Beträge aller Wurzeln von $f(\varrho)$ und alle Wurzeln dieses Betrages II, 216

ϱ_1	von	der	Vielfachheit	r
$-\varrho_1$	"	"	"	r_0
$\varrho_1 e^{\pm i\varphi_1}$	"	"	"	r_1

$(r + r_0 + 2r_1 \leqq 3)$. Dann ist

$$\frac{\sum \varrho^{\nu+1}}{\sum \varrho^{\nu}} = \frac{r\varrho_1^{\nu+1} + r_0(-1)^{\nu+1}\varrho_1^{\nu+1} + 2r_1\cos(\nu+1)\varphi_1\varrho_1^{\nu+1} + \sum' \varrho^{\nu+1}}{r\varrho_1^{\nu} + r_0(-1)^{\nu}\varrho_1^{\nu} + 2r_1\cos\nu\varphi_1\varrho_1^{\nu} + \sum' \varrho^{\nu}}$$

wo $\sum'$ über die ev. noch vorhandenen Wurzeln von kleinerem Betrage geht, also

$$\frac{\sum \varrho^{\nu+1}}{\sum \varrho^{\nu}} = \varrho_1 \frac{r + (-1)^{\nu+1}r_0 + 2\cos(\nu+1)\varphi_1 \cdot r_1 + \varepsilon_{\nu+1}}{r + (-1)^{\nu}r_0 + 2\cos\nu\varphi_1 \cdot r_1 + \varepsilon_{\nu}},$$

wo $\lim\limits_{\nu=\infty} \varepsilon_\nu = 0$. Nun läßt sich κ so wählen, daß $\kappa\varphi_1 \mod \pi$ beliebig klein wird, und zwar beliebig oft. Setzt man dann $\nu = 2\kappa$, so geht für solche ν $\cos\nu\varphi_1$ gegen 1, $\cos(\nu+1)\varphi_1$ gegen $\cos\varphi_1$ und daher obiger Ausdruck gegen

$$\varrho_1 \frac{r - r_0 + 2r_1\cos\varphi_1}{r + r_0 + 2r_1}$$

Setzt man aber $\nu = 2\kappa - 1$, so konvergiert der Ausdruck gegen II, 217

$$\varrho_1 \frac{r + r_0 + 2r_1}{r - r_0 + 2r_1\cos\varphi_1}$$

Beide Ausdrücke sollen gleich ϱ' sein, und da ϱ' als Quotient positiver Zahlen positiv ist, auch positiv:

$$\frac{r + r_0 + 2r_1}{r - r_0 + 2r_1\cos\varphi_1} = \frac{r - r_0 + 2r_1\cos\varphi_1}{r + r_0 + 2r_1} > 0$$

also $r - r_0 + 2r_1 \cos\varphi_1 = r + r_0 + 2r_1$,

$$2r_0 - 2r_1 \cos\varphi_1 + 2r_1 = 0$$
$$r_0 + r_1(1 - \cos\varphi_1) = 0$$

d. h.

$$r_0 = 0\,, \quad r_1 = 0.$$

Es ist also $r > 0$ und ϱ_1 positive Wurzel und

$$\varrho' = \lim_{\nu=\infty} \frac{\sum \varrho^{\nu+1}}{\sum \varrho^{\nu}} = \varrho_1\,.$$

ϱ_1 ist „größte positive Wurzel“, und als solche mit ϱ_0 identisch. Also

$$\varrho' = \varrho_0\,, \qquad \text{w. z. b. w.}$$

Überdies folgt noch, daß ϱ_0 nicht nur als größte positive Wurzel, sondern auch als Wurzel von von größtem absoluten Betrage charakterisiert ist. Denn nach dem Beweise haben alle anderen Wurzeln kleineren Betrag als $\varrho_1 = \varrho' = \varrho_0$.

II, 218

Satz 12. *Sind x_0, x_1, x_2 drei linear unabhängige Elemente eines reellen kubischen Körpers K, deren Jacobi–Algorithmus n–zeilig rein periodisch ist, so hat die charakteristische Gleichung eine bestimmte, positive Wurzel ϱ_0, die die beiden anderen an Betrag übertrifft. ϱ_0 ist (primitives) Element von K und Einheit von K. Es gelten die Relationen*

$$\varrho_0 x_i = \sum_{\kappa=0}^{2} \mathsf{A}_i^{(n+\kappa)} x_\kappa$$

und

$$x_2 : x_1 : x_0 = g_{2,\kappa}(\varrho_0) : g_{1,\kappa}(\varrho_0) : g_{0,\kappa}(\varrho_0)$$

wobei

$$g_{i,\kappa}(\varrho_0) = \mathsf{A}_i^{(\kappa)} \varrho^2 + \left(\mathsf{A}_i^{(n+\kappa)} - b_1 \mathsf{A}_i^{(\kappa)}\right) \varrho + \\ + \left(\mathsf{A}_i^{(2n+\kappa)} - b_1 \mathsf{A}_i^{(n+\kappa)} - b_2 \mathsf{A}_i^{(\kappa)}\right)$$

ist, wenn

$$f(\varrho) = \varrho^3 - b_2 \varrho^2 - b_1 \varrho - 1$$

die charakteristische Gleichung ist.

Beweis: Es ist nur noch das letztere zu zeigen. Dazu benutzen wir die Relation von Satz 9 für $\nu = 1$.[1]

II, 211*

$$\frac{g_{i,\kappa}(\varrho)}{f(\varrho)} = \sum_{\mu=0}^{\infty} \frac{\mathsf{A}_i^{(\mu n+\kappa)}}{\varrho^{\mu+1}}\,,$$

multiplizieren mit $f(\varrho)$, dann müssen alle negativen Potenzen herausfallen, da $g_{i,\kappa}(\varrho)$ ganz. Die Ausmultiplikation ergibt dann die im Satz genannten Ausdrücke.

25. 1. 62

$$1, \sqrt[3]{2}, \sqrt[3]{2}^2 \quad \text{hat} \quad \left\{ \begin{array}{cc} \text{Vorperiode} & \left\{\begin{matrix}1 & 1\\ 2 & 3\end{matrix}\right\} \\ \text{Periode} & \begin{matrix}3 & 3\end{matrix} \end{array} \right\}$$

$$1, \sqrt[3]{2}^2, \sqrt[3]{2} \quad \text{hat} \quad \left\{ \begin{array}{cc} \text{Vorperiode} & \begin{matrix}1 & 1\end{matrix} \\ \text{Periode} & \left\{\begin{matrix}0 & 1\\ 1 & 2\end{matrix}\right\} \end{array} \right\}$$

Bei $\sqrt[3]{2}, \sqrt[3]{2}^2, 1$ ist nach 4 Schritten noch keine Periode erkennbar.

3. 2. 62

$$1, \sqrt[3]{3}, \sqrt[3]{3}^2 \quad \text{hat} \quad \left\{ \begin{array}{cc} \text{Vorperiode} & \left\{\begin{matrix}1 & 2\\ 0 & 2\end{matrix}\right\} \\ \text{Periode} & \left\{\begin{matrix}1 & 5\\ 1 & 2\end{matrix}\right\} \end{array} \right\}$$

II, 212*

f.) Reduziertheitsbedingung für gewöhnliche Kettenbrüche in Matrizenschreibweise

(Besprechung mit Toeplitz am 17. XII. 23).

Ist $f(x) = 0$ eine in irgendeinem Körper K irreduzible Gleichung, so läßt sich der algebraische Körper $K(\mathfrak{o})$ isomorph in Matrizen darstellen (Kronecker). Ist nämlich $x_1, \ldots, x_n$ ein System von n linear unabhängigen Elementen aus

[1] Hasse numeriert die folgenden Seiten mit 211, 212, ..., 219. Zur Vermeidung von Verwechslungen fügen wir jeweils einen Stern an, schreiben also 211*,... 219*.

$K(x)$ (Grad n), erhält man die Hauptgleichung eines primitiven Elementes, etwa x bekanntlich als charakteristische Gleichung derjenigen Matrix A, die die Vielfachen xx_i durch die x_κ darstellt, in der Form

$$f(x) \equiv |x\mathsf{E} - \mathsf{A}|$$

Die Matrix A hat Koeffizienten in K. Übergang zu einer anderen Basis bedeutet Transformation von A in eine ähnliche Matrix $\mathsf{S}^{-1}\mathsf{AS}$ vermöge einer Matrix S nicht verschwindender Determinante aus K. Die Determinante von A verschwindet als Norm von x nicht. Wir führen für die Elemente $y = \varphi(x)$ in ganz–rationaler Darstellung folgende Abbildung auf einen Matrizenbereich $\overline{K}$ aus:

$$\varphi(x) \longleftrightarrow \varphi(\mathsf{A}).$$

Nach einem Satz von Frobenius genügt A seiner eigenen charakteristischen Gleichung:

$$f(\mathsf{A}) = 0$$

und wenn (wie hier der Fall) $f(x)$ irreduzibel in K, also keine mehrfachen Wurzeln hat (vollkommener Körper!), keiner niedrigeren Gleichung. Dadurch ist die Isomorphie von $K(x)$ mit $\overline{K}$ erwiesen. II, 213*

Die Matrizen von $\overline{K}$, d. h. die Gesamtheit aller $\varphi(\mathsf{A})$ bilden einen Körper, der als Darstellung von $K(x)$ durch Matrizen bezeichnet werden kann. Diese Darstellung macht keinen Unterschied zwischen den n konjugierten Wurzeln von $f(x)$.

II, 214* Alle Matrizen von $\overline{K}$ sind untereinander vertauschbar entweder wegen der Isomorphie oder der Darstellung $\varphi(\mathsf{A})$. Sie liegen sämtlich in K.

Ist $\mathsf{B} = \varphi(\mathsf{A})$ eine Matrix von $\overline{K}$ und $y = \varphi(x)$ das entspr. Element von $K(x)$, hat ersichtlich y die Darstellungsmatrix $\mathsf{B} = \varphi(\mathsf{A})$ durch x_1, x_2, also ist die Hauptgleichung für A die charakteristische Gleichung von B. Daher sind die Determinanten aller von Null verschiedenen Matrizen B aus $\overline{K}$ ungleich Null, als Normen der zugeordneten $y \neq 0$.

Ist irgendein Körper von Matrizen in K gegeben, der in obigem Sinne zu $K(x)$ isomorph ist, und A die x entsprechende Matrix, so muß $f(\mathsf{A}) = 0$ die irreduzible Gleichung sein, der A genügt, d. h. $f(x)$ ist die charakteristische

Gleichung von A. Das System

$$\begin{array}{rrcl} & x_1 x & = & a_{11}x_1 + a_{12}x_2 + \cdots \\ & x_2 x & = & a_{21}x_1 + a_{22}x_2 + \cdots \\ & \vdots & & \ldots\ldots \\ \text{kurz} & x(x_i) & = & \mathsf{A}(x_i) \end{array}$$

hat dann wegen $|x\mathsf{E} - \mathsf{A}| \equiv f(x) = 0$ eine Lösung $x_1, \ldots, x_n$, die von Null verschieden ist. Diese Lösung liegt in $K(x)$ und ihre Elemente müssen linear unabhängig in $K(x)$ sein (Folgt aus der Irreduzibilität von $f(x)$*). Sie sind daher eine Basis von $K(x)$. Daher entsteht unsere Darstellung notwendig auf obige Weise. Daraus folgt:

Satz 1. *Zwei verschiedene Darstellungen eines algebraischen Körpers $K(x)$ durch Matrizen in K sind ähnlich in K.*

Ohne auf den vollständigen Beweis dieses Satzes im allgemeinen Falle einzugehen (Ergänzung der in der letzten Anmerkung berührten Lücke), will ich ihn nur für $n = 2$ erbringen. II, 215*

Sei

$$\mathsf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

so ist

$$x\mathsf{E} - \mathsf{A} = \begin{pmatrix} a_{11} - x & a_{12} \\ a_{21} & a_{22} - x \end{pmatrix}$$

und

$$f(x) = |x\mathsf{E} - \mathsf{A}| = x^2 - (a_{11} + a_{22})x + |\mathsf{A}|$$

Die Lösung des Gleichungssystems

$$\begin{array}{rcl} xx_1 & = & a_{11}x_1 + a_{12}x_2 \\ xx_2 & = & a_{21}x_1 + a_{22}x_2, \end{array}$$

* denn die x_i sind als Unterdeterminanten von $|x\mathsf{E} - \mathsf{A}|$ vom Grade $(n-1)$ in x

wenn $f(x) = 0$, hat die Form

$$x_1 : x_2 = a_{12} : (x - a_{11}) = (x - a_{22}) : a_{21}$$

Wäre a_{12} oder $a_{21} = 0$, so wäre $x = a_{22}$ oder a_{11}, also $f(x)$ nicht irreduzibel. Daher kann z. B.

$$\begin{aligned} x_1 &= a_{12} \\ x_2 &= x - a_{11} \end{aligned}$$

genommen werden, und dies ist wegen $\begin{vmatrix} a_{12} & 0 \\ -a_{11} & 1 \end{vmatrix} = a_{12} \neq 0$ gleichzeitig mit $(1, x)$ ein System linear unabhängiger Größen. (Ähnlich muß der Beweis für beliebiges n verlaufen).

Ich beweise jetzt:

II, 216*

Satz 2. *Sind* A, B *zwei linear unabhängige Matrizen einer rationalen Darstellung eines reell quadratischen Zahlkörpers über* R*, so ist der Basisquotient des* A, B *entsprechenden zweigliedrigen Moduls, d. h. die dem Quotienten* $\frac{\mathsf{B}}{\mathsf{A}} = C$ *entsprechende quadratische Irrationalzahl dann und nur dann reduziert, wenn folgende* 3 *Bedingungen bestehen:*

1.) $|C + \mathsf{E}| > 0,$

2.) $|C - \mathsf{E}| < 0,$

3.) $|C| < 0.$

Beweis: Von vorneherein ist zu sagen, daß diese Bedingungen der notwendigen Anforderung genügen, gegen Transformation mit beliebigen Matrizen S aus R invariant zu sein.

Sei nun α das C entsprechende Element und

$$a\alpha^2 - b\alpha - c = 0\,; \quad (a > 0)$$

die ganzzahlige primitive, eindeutig bestimmte Gleichung, der α genügt, mit der Diskriminante

$$D = b^2 + 4ac \neq 0.$$

Sei ferner $\sqrt{D}$ die positive Wurzel und

$$\begin{aligned} \alpha &= \frac{b+\sqrt{D}}{2a} \\ \alpha' &= \frac{b-\sqrt{D}}{2a}. \end{aligned}$$

Aus den notwendigen und hinreichenden Bedingungen

$$\alpha > 1, \quad -\frac{1}{\alpha'} > 1$$

für reduzierte α folgt als gleichwertig die Ungleichungsfolge

$$0 < \sqrt{D} - b < 2a < \sqrt{D} + b,$$

(aus der übrigens folgt $b > 0$ und somit $\sqrt{D} > 0$, sodaß nur dasjenige von α, α' als reduziert in Frage kommt, dessen $\sqrt{D} > 0$ ist).

Nun ist offenbar

$$C = \frac{1}{2a}\begin{pmatrix} b & 1 \\ D & b \end{pmatrix}$$

eine α in einer rationalen Darstellung entsprechende Matrix, wenn nämlich als Basis $1, \sqrt{D}$ zugrundegelegt wird. II, 217*

1.) Die Bedingungen 1.) − 3.) für C ergeben:

1.) $(b + 2a)^2 - D > 0$

2.) $(b - 2a)^2 - D < 0$

3.) $b^2 - D < 0$.

Aus 3.) folgt $|b| < \sqrt{D}$, aus 1.) u. 2.) $|b + 2a| < \sqrt{D}$,

$$|2a - b| = |b - 2a| < \sqrt{D},$$

also sicher $|2a + b| > |2a - b|$, d. h. wegen $a > 0$ auch $b > 0$, d. h.

$$b < \sqrt{D}$$

$$2a + b > \sqrt{D} > 2a - b,$$

einerlei ob $2a - b \gtrless 0$ ist. Das ergibt

$$0 < \sqrt{D} - b < 2a < \sqrt{D} + b,$$

also die Reduziertheit.

2.) Umgekehrt folgt aus jenen Ungleichungen durch Quadrieren:

$$\begin{gathered} b^2 - D < 0 \\ (2a - b)^2 - D < 0 \\ (2a + b)^2 - D > 0, \end{gathered}$$

was mit 1.), 2.), 3.) gleichwertig.

Wegen der Invarianz gegen Transformation der Darstellung ist damit der Beweis erbracht.

2.3 Frobeniusscher Satz über die charakteristische Gleichung. (20.1.1924)

Bôcher's proof of the theorem of Frobenius on the characteristic polynomial of a matrix [Bôc07]. *The theorem says that every matrix is a root of its characteristic poynomial. Compare also section c) of the preceeding entry.*

II, 218*

(Beweis nach Bôcher)

20. I. 1924.

Satz. *Ist A eine beliebige Matrix und*

$$\varphi(\lambda) = |A - \lambda E| = 0$$

ihre charakteristische Gleichung, so gilt

$$\varphi(A) = 0.$$

Beweis: Sei $C(\lambda) = A - \lambda E$ die charakteristische Matrix und $\overline{C}(\lambda)$ ihre Adjungierte, die als ganze rationale Funktion vom Grade $n-1$ in λ mit Matrizenkoeffizienten angesehen werden kann, wenn n der Grad von A ist. Nach Definition der Adjungierten ist dann

$$C(\lambda)\overline{C}(\lambda) = |C(\lambda)|E = \varphi(\lambda)E.$$

Die Matrix $\varphi(\lambda)E$ kann offenbar auch als $\varphi(\lambda E)$ geschrieben werden. Denn ist

$$\varphi(\lambda) = \sum_{\nu=0}^{n} c_\nu \lambda^\nu$$

so ist $\varphi(\lambda)E$ die Matrix

$$\varphi(\lambda)E = \begin{pmatrix} \sum_{\nu=0}^{n} c_\nu \lambda^\nu & & & \\ & \sum_{\nu=0}^{n} c_\nu \lambda^\nu & & \\ & & \ddots & \\ & & & \sum_{\nu=0}^{n} c_\nu \lambda^\nu \end{pmatrix} = \sum_{\nu=0}^{n} c_\nu (\lambda^\nu E^\nu) = \varphi(\lambda E)$$

Aus obiger Gleichung folgt also durch Einsetzen von $C(\lambda) = A - \lambda E$:

$$(A - \lambda E)\overline{C}(\lambda) = \varphi(\lambda E).$$

II, 219* Hiernach ist $A - \lambda E$ ein Linearfaktor von $\varphi(\lambda E)$ für variables λ. Daraus folgt elementar algebraisch (Koeffizientenvergleich nach λ), daß auf

$$\varphi(A) = 0$$

geschlossen werden darf.

Der Schluß verläuft genau so: Sei $\overline{C}(\lambda) = \sum_{\nu=0}^{n-1} C_\nu \lambda^\nu$
Dann ist

$$\begin{aligned}(A - \lambda E)\overline{C}(\lambda) &= \sum_{\nu=0}^{n-1} AC_\nu \lambda^\nu - \sum_{\nu=1}^{n} C_{\nu-1}\lambda^\nu \\ &= \sum_{\nu=1}^{n-1}(AC_\nu - C_{\nu-1})\lambda^\nu + AC_0 - C_{n-1}\lambda^n\end{aligned}$$

also das Gleichungssystem

$$\begin{array}{rcl} AC_0 &=& c_0 E \\ AC_1 - C_0 &=& c_1 E \\ \multicolumn{3}{c}{\dotfill} \\ AC_{n-1} - C_{n-2} &=& c_{n-1} E \\ -C_{n-1} &=& c_n E \end{array}$$

wenn $\varphi(\lambda) = \sum_{\nu=0}^{n} c_\nu \lambda^\nu$ gesetzt ist. Durch Multiplikation mit den A Potenzen und Addition folgt dann:

$$\sum_{\nu=0}^{n} c_\nu A^\nu = 0\,, \quad \text{d. h.} \quad \varphi(A) = 0\,, \qquad \text{w. z. b. w.}$$

Kapitel 3

Tagebuch III: Mai 1924 – Oktober 1925

Eintragungen

3.1 Definition abstrakter Gruppen durch Relationen. (2.5.1924)

Abstract groups may be defined by giving generators and relations. Hasse notes that he has learned this from Schreier. Since 1924 the group theorist Otto Schreier was in Hamburg and worked in close contact with Artin. During those years Hasse often went to Hamburg in order to participate there at seminars and colloquium talks.

III, 3

2. V. 24.

(Dehnsche Auffassung, nach Schreier, Hamburg, März 1924)

Gegeben seien irgendwelche (endlich oder unendlich viele) Zeichen $a_1, a_2, \ldots$, denen wir die Zeichen $a_1^{-1}, a_2^{-1}, \ldots$ hinzufügen. Wir betrachten dann (endliche) „Worte" aus jenen Zeichen, z. B.

$$A = a_1 a_2^{-1} a_1^{-1} a_2^{-1} a_2^{-1} a_2^{-1} a_2 a_1 a_1 a_1 a_2$$

etz. Als erlaubte „Verwandlungen" bezeichnen wir das Einschieben oder Weglassen von den speziellen Worten

$$\begin{array}{lll} a_1 a_1^{-1}, & a_2 a_2^{-1}, & \ldots\ldots \\ a_1^{-1} a_1, & a_2^{-1} a_2, & \ldots\ldots \end{array}$$

Zwei Worten heißen „gleich", wenn sie durch solche Verwandlungen ineinander überführbar sind, speziell ist also:

$$a_1 a_1^{-1} = a_1^{-1} a_1 = 1, \ldots$$

wo 1 das zeichenlose Wort bezeichnet.

Zwei Worte lassen sich komponieren, indem man sie hintereinander schreibt. Diese Komposition ist assoziativ, dagegen nicht kommutativ. Nicht trivial ist die Eindeutigkeit der Komposition, die auf den Nachweis

$$AB = AB', \quad \text{wenn} \quad B = B'$$

zurückkommt, und die Unabhängigkeit des Produktes von der Schreibweise der Faktoren–Worte behauptet. Kann man aber B durch erlaubte Abänderung in

III, 4 B' verwandeln, so gilt dasselbe natürlich von AB in AB'. Es ist somit jedem Wortpaar A, B ein eindeutig bestimmtes Wort, sein Kompositum AB zugeordnet, die Komposition ist assoziativ, ferner existiert ein „Einheitswort", das zeichenlose 1, und zu jedem Wort ein reziprokes, z. B. zu a_1: a_1^{-1}, zu $a_1 a_2$: $a_2^{-1} a_1^{-1}$ etz., daß durch erlaubte Abänderung aus AA^{-1} die 1 entsteht. Also gilt:

Satz 1. *Die aus beliebig vielen Zeichen $a_1, a_2, \ldots$ und den „reziproken" $a_1^{-1}, a_2^{-1}, \ldots$ gebildeten Worte, von denen zwei dann und nur dann gleich heißen, wenn sie durch Einschiebung oder Fortlassung von $a_1 a_1^{-1}, \ldots a_1^{-1} a_1 \ldots$ entstehen, bilden bezüglich der Hintereinandersetzung als Komposition eine Gruppe. Diese heißt die freie Gruppe $\mathfrak{F}$ der Erzeugenden $a_1, a_2, \ldots$*

Seien nun irgendwelche Worte $\mathsf{R}_1, \mathsf{R}_2, \ldots$ dieser freien Gruppe $\mathfrak{F}$ gegeben (endlich oder unendlich viele), dann betrachten wir alle aus ihnen durch beliebige Komposition zu bildenden Worte, sowie alle von der Form $\mathsf{S}^{-1}\mathsf{R}\mathsf{S}$, wo S irgendein Wort der freien Gruppe ist, und R schon durch Komposition oder in derselben Art enthalten ist, kurz gesagt alle Worte, die sich durch unbeschränkte Komposition und Transformation der komponierten Worte mit Elementen der freien Gruppe, sowie erneute Komposition etz. herleiten lassen. Diese bilden ersichtlich eine Gruppe von Worten, die in der freien Gruppe enthalten ist.
III, 5 Diese Untergruppe ist ferner Normalteiler $\mathfrak{R}$ von $\mathfrak{F}$. Ihre Nebengruppen bilden also eine Gruppe $\mathfrak{G}$, die Faktorgruppe $\mathfrak{F}/\mathfrak{R}$.

Diese Faktorgruppe $\mathfrak{G}$ besteht aus allen Worten von $\mathfrak{F}$ mit der Bestimmung, daß alle und nur die Worte von $\mathfrak{R}$ gleich dem zeichenlosen Wort 1 gesetzt werden sollen. In $\mathfrak{G}$ liegt also eine Gruppe vor, die aus den Erzeugenden $a_1, a_2, \ldots$ gebildet ist, und in der alle und nur die Relationen $\mathsf{R} = 1$ bestehen, die aus dem System $\mathsf{R}_1, \mathsf{R}_2, \ldots$ durch Komposition und Transformation innerhalb $\mathfrak{F}$ (also in trivialer Weise) folgen.

Satz 2. *Die Gruppe $\mathfrak{G}$, die aus $a_1, a_2, \ldots$ erzeugt wird, und in der alle und nur die Relationen $\mathsf{R}_1 = \mathsf{R}_2 = \cdots = 1$ mit ihren trivialen Folgen gelten, läßt sich charakterisieren als die Faktorgruppe $\mathfrak{F}/\mathfrak{R}$ von $\mathfrak{F}$ bezüglich desjenigen Normalteilers $\mathfrak{R}$ von $\mathfrak{F}$, der aus allen Worten $\mathsf{R}_1, \mathsf{R}_2, \ldots$ von $\mathfrak{F}$ bei unbeschränkter Komposition und Transformation innerhalb $\mathfrak{F}$ erzeugt wird.*
III, 6

Diese Schlußweise läßt sich verallgemeinern (Schreier), wenn für die unendlichen zyklischen Gruppen $a_1^n, a_2^n, \ldots$ als deren „freies Produkt" $\mathfrak{F}$ erscheint,

irgendwelche Gruppen $\mathfrak{G}_1, \mathfrak{G}_2, \ldots$ gegeben sind, die je aus verschiedenen (freien) Elementen erzeugt werden. Dann gelangt man so zur Konstruktion des „freien Produkts“ der $\mathfrak{G}_1, \mathfrak{G}_2, \ldots$

3.2 Zum Kirkmannschen Dreierproblem für $n = 15$. (2.5.1924)

Kirkman's combinatorial problem of order 15 is as follows: Fifteen girls in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast. Hasse notes Schreier's contribution to this problem which works with the elementary abelian group of order 16. See also the entry of 26 September 1927 in Book IV.] We observe that in the summer semester 1924 Toeplitz in Kiel had announced a lecture "for students of all faculties who love mathematics". The young Hasse was close to Toeplitz during these years and surely they have talked about the topics for such a lecture. It may well have been that Kirkman's problem was discussed in this context.

III, 7

2. V. 24.

(Nach Schreier, Hamburg, März 1924).

Wir identifizieren die 15 Damen des Kirkmannschen Problems mit den 15 Elementen $\neq 1$ der Abelschen Gruppe vom Typus $(2, 2, 2, 2)$, gegeben durch ihre Basisdarstellung

$$s_{x_1,x_2,x_3,x_4} = s_1^{x_1} s_2^{x_2} s_3^{x_3} s_4^{x_4}\,; \quad (x_i \mod 2).$$

Diese Gruppe hat genau 35 Untergruppen der Ordnung 4. Denn je zwei Elemente $\neq 1$ bestimmen eine solche Vierergruppe eindeutig. Es gibt $\binom{15}{2} = 105$ solche Paare, von denen je 3 die gleiche Untergruppe bestimmen.

Die 35 Untergruppen stellen, wenn man nur ihre Elemente $\neq 1$ betrachtet ein System von 35 Dreiern dar, wobei jedes der 15 Elemente $\neq 1$ mit jedem anderen in genau einem Dreier vorkommt, da einerseits jedes Elementepaar $\neq 1$ in einer Untergruppe d. Ordn. 4 vorkommen muß, andererseits aber auch in nur einer, da sein Produkt das dritte Element jener Vierergruppe eindeutig bestimmt.

Es kommt also zur Lösung des Kirkmannschen Problems nur darauf an, diese 35 Dreier so in 7 Systeme zu je 5 zu verteilen, daß in jedem System jedes Element $\neq 1$ genau einmal steht. Hierzu bemerken wir, daß $\mathfrak{G}$ genau III, 8

$$(2^4 - 1)(2^4 - 2)(2^4 - 4)(2^4 - 8) \equiv 0 \mod 7$$

Automorphismen, also sicher einen Automorphismus der Ordnung 7 hat. Da 7 auch nur einmal in der Ordnung dieser Automorphismengruppe aufgeht, folgt nach dem Sylowschen Satz sogar:

Ist σ ein Automorphismus der Ordnung 7 von $\mathfrak{G}$, so sind die Perioden aller Automorphismen der Ordnung 7 zur Periode von σ in $\mathfrak{G}$ konjugiert, d. h. es gilt für jeden andern Automorphismus σ' der Ordnung 7 eine Darstellung

$$\sigma' = \alpha^{-1}\sigma^{\nu}\alpha$$

wo α irgendein Automorphismus von $\mathfrak{G}$ ist. Die durch σ' bewirkte Permutation der Elemente von $\mathfrak{G}$ entsteht also aus der durch σ^{ν} bewirkten lediglich durch Umbenennung der permutierten Elemente von $\mathfrak{G}$.

Man findet leicht den folgenden Automorphismus σ der Ordnung 7:

$$\begin{array}{lcl} s_1 & \longrightarrow & s_1 \\ s_2 & \longrightarrow & s_3 \\ s_3 & \longrightarrow & s_4 \\ s_4 & \longrightarrow & s_1 s_2 s_4\,, \end{array}$$

bei dessen Konstruktion man zweckmäßig benutzt, daß σ nicht eine Untergruppe der Ordnung 4 invariant lassen kann, und daher, wie leicht zu sehen aus 2 siebengliedrigen Zyklen und 1 festen Element s_1 bestehen muß. Hier ist

$$\sigma = (s_2, s_3, s_4, s_{124}, s_{234}, s_{123}, s_{134})(s_{1234}, s_{23}, s_{34}, s_{12}, s_{13}, s_{14}, s_{24})$$

Auf Grund von $\sigma, \sigma^2, \ldots \sigma^7 = 1$ zerfallen nun die 35 Vierergruppen in 5 Systeme zu je 7, sodaß jedes System immer durch $\sigma, \sigma^2, \ldots \sigma^7 = 1$ aus seiner ersten Untergruppe entsteht. Indem ich nur die Ziffern schreibe, erhält man so:

III, 9

$\underline{1}$	$\underline{2}$	$\underline{12}$	2	3	23	2	4	24	12	13	23	3	12	123
1	3	13	3	4	34	3	124	1234	13	14	34	4	13	134
1	4	14	4	124	12	4	234	23	14	24	12	124	14	2
1	124	24	$\underline{124}$	$\underline{234}$	$\underline{13}$	124	123	34	24	1234	13	234	24	3
1	234	1234	234	123	14	234	134	12	1234	23	14	$\underline{123}$	$\underline{1234}$	$\underline{4}$
1	123	23	123	134	24	123	2	13	$\underline{23}$	$\underline{34}$	$\underline{24}$	134	23	124
1	134	34	134	2	1234	$\underline{134}$	$\underline{3}$	$\underline{14}$	34	12	1234	2	34	234

Nun hat man lediglich noch in jeder Spalte eine Untergruppe so auszuwählen, daß diese 5 Untergruppen genau alle Elemente umfassen. Von da an liefert dann zyklisches Fortgehen (Anwendung von σ) die gesuchte Lösung. Eine solche ist oben durch Unterstreichen angedeutet.

Die Anzahl der so entstehenden Lösungen läßt sich leicht abzählen. Andere Automorphismen braucht man nicht zu berücksichtigen, sie führen nur auf Umbenennung. Ob die aus obiger Tabelle entstehenden Lösungen durch Umbenennung äquivalent sind, und ob ev. noch weitere Lösungen existieren, vermag ich nicht zu entscheiden.

3.3 Bemerkung zur Topologie. (2.5.1924)

The topological product of two circles is a torus, and the product of two circles modulo their order is a Moebius strip. Artin had explained this to Hasse when the latter had visited Hamburg. In the years 1924/25 Artin was working in topology and had two topological papers in the Hamburger Abhandlungen.

III, 10

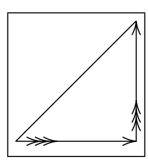
2. V. 24.

(Nach Bemerkung von Dr. Artin, Hamburg, März 1924)

Bekanntlich ist das Produkt von 2 Kreismannigfaltigkeiten ein Torus (Normales Querschnittsystem als Koordinaten). Wie steht es aber mit dem Produkt von 2 Kreisen, wenn man von der Reihenfolge absieht? Was damit gemeint ist mag man sich an der Uhr verdeutlichen. Der erste Fall wird geliefert durch alle Stellungen der beiden Uhrzeiger, der zweite durch alle Stellungen zweier nicht unterschiedener Uhrzeiger.
Behauptung: *Im zweiten Falle ist die Produktmannigfaltigkeit ein Möbiussches Band.*
Beweis: Deutet man die Punkte der 2 Kreise in einem Bildkoordinatensystem durch die Größe ihrer Zentriwinkel auf 2 Achsen, so erhält man zunächst ohne Nebenbedingung ein dem Torus äquivalentes Quadrat:

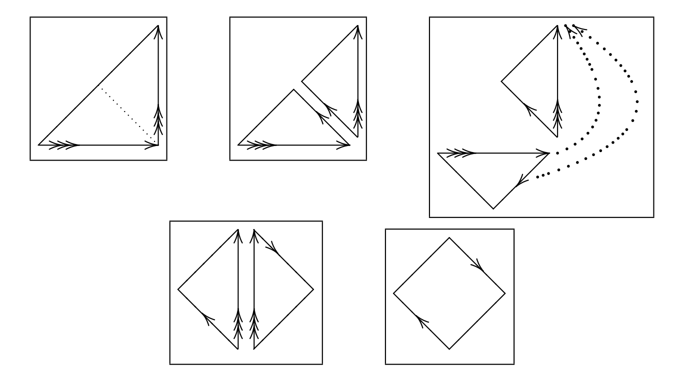


Nun führen wir die Nebenbedingung ein, wodurch sich das Quadrat auf seine eine Hälfte mit folgender Randzuordnung reduziert



Diese Zuordnung wird wie folgt durch Zerschneiden und aneinanderlegen realisiert:

III, 11



Man sieht hiernach direkt, daß das Möbiussche Band entsteht, nämlich ein Quadrat mit 2 gegenüberliegenden, in entgegengesetztem Sinne identischen Seiten und 2 freien Rändern. Die freien Ränder entsprechen übrigens den zusammenfallenden Stellungen der beiden Uhrzeiger.

3.4 Literatur zur komplexen Multiplikation, speziell Bernoullische Zahlen in imag. quadr. Körpern (2.5.1924)

Literature on complex multiplication, in particular generalized Bernoulli numbers in complex quadratic number fields.

III, 12

2. V. 24.

(Nach Hecke, Hamburg, März 1924)

Klein–Fricke, Modulfunktionen

Fricke, Enzyklopädie–Artikel

Hurwitz, Ann. **51**

Dienzl, Matter: Wiener Ber. 1909
Monatshefte f. Math. u. Phys. XXV, 1914.

3.5 Die logarithmischen Differentialquotienten Kummers in gewissen Oberkörpern des Kreiskörpers k_ζ. (27.5.1924)

Kummer's logarithmic differential quotients in extensions of cyclotomic fields, and their appearance in explicit formulas for the Hilbert symbol. Compare with the entry of July 21, 1923 in Book I.]

III, 13

27. V. 24.

Sei K ein solcher Oberkörper von k_ζ, in dem der Primteiler $\mathfrak{l}_0 = (\lambda) = (1-\zeta)$ von k_ζ einen Primteiler $\mathfrak{l}$ der Ordnung 1 hat, f der Grad von $\mathfrak{l}$, w eine primitive $(\ell^f - 1)$–te Einheitswurzel von $K(\mathfrak{l})$. Dann ist

$$K(\mathfrak{l}) = k_\zeta(\mathfrak{l}, w) = R(\ell, \zeta, w)$$

der Körper der $\ell(\ell^f - 1)$–ten Einheitswurzeln vom Grade ℓf über dem Körper $R(\ell)$ der rationalen ℓ–adischen Zahlen, also Abelsch und komponiert als:

$$K(\mathfrak{l}) = \big\{R(\ell, \zeta), R(\ell, w)\big\}.$$

Seine Gruppe ist das direkte Produkt der Gruppen:

$$s, s^2, \dots, s^{\ell-1} = 1; \quad s = (\zeta : \zeta^r); \quad r \text{ prim. } (\ell-1)\text{–te E. W. aus } R(\ell).$$
$$\sigma, \sigma^2, \dots, \sigma^f = 1; \quad \sigma = (w : w^\ell).$$

$R(\ell, w)$ ist der Koeffizientenkörper von $K(\mathfrak{l})$.

Es sei nun $\alpha = \varphi(\zeta) \equiv 1 \text{ mod. } \mathfrak{l}$ irgendein Element von $K(\mathfrak{l})$ in einer Darstellung als Funktion von ζ mit Koeffizienten aus $R(\ell, w)$. Dann betrachten wir die α zugeordnete Funktion $\varphi(e^v)$ für Argumente

$$v \equiv 0 \text{ mod. } \ell$$

aus $R(\ell, w)$. e^v und somit $\varphi(e^v)$ haben einen Sinn für diese Argumente, falls der Nenner von $\varphi(e^v)$ nicht verschwindet. Wir können aber die Funktion $\varphi(e^v)$ stets so voraussetzen. Dann ist

III, 14

$$\alpha = \varphi(\zeta) = \frac{g(\zeta)}{h(\zeta)}$$

so als Quotient zweier ganzen rationalen in $R(\ell, w)$ ganzzahligen Funktionen g und h von ζ dargestellt, daß

$$g(\zeta) \quad \text{und} \quad h(\zeta) \quad \text{prim zu} \quad \mathfrak{l}$$

sind, so folgt aus

$$\begin{aligned} h(\zeta) &\equiv h(1) \ \text{mod.}\, \mathfrak{l} \\ h(e^v) &\equiv h(1) \ \text{mod.}\, \ell, \quad (\text{für } v \equiv 0 \ \text{mod.}\, \ell) \end{aligned}$$

daß, wenn $h(e^v)$ durch ℓ teilbar wäre, es auch $h(1)$ und also $h(\zeta)$ durch $\mathfrak{l}$ teilbar, was wir ausschlossen.
Sei also φ so vorausgesetzt. Dann ist

$$\varphi(e^v) = \frac{g(e^v)}{h(e^v)} \equiv \frac{g(1)}{h(1)} = \varphi(1) \ \text{mod.}\, \ell,$$

weil $h(1)$ und $h(e^v)$ prim zu ℓ sind, und weiter

$$\varphi(e^v) \equiv \varphi(1) \equiv 1 \ \text{mod.}\, \ell,$$

weil

$$g(1) \equiv g(\zeta) \equiv \alpha h(\zeta) \equiv h(\zeta) \equiv h(1) \ \text{mod.}\, \ell$$

und

$$\varphi(1) = \frac{g(1)}{h(1)}$$

ist.

Somit ist für alle $v \equiv 0$ mod. ℓ aus $R(\ell, w)$

$$\log \varphi(e^v) = \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} \big(\varphi(e^v) - 1\big)^{\nu}; \quad (\ell)$$

konvergent und definiert ein bestimmtes Element aus $R(\ell, w)$. Dieser Logarithmus genügt ferner nach Hensel den bekannten Funktionalgleichungen.

III, 15

Wir interessieren uns hier nicht für die Funktionswerte von $\log \varphi(e^v)$, sondern für die Koeffizienten der Reihenentwicklung nach Potenzen von v in der Umgebung der (im Konvergenzgebiet gelegenen) Stelle $v = 0$. Allgemein gilt hier:

$$\text{Koeffizient von } \frac{v^a}{a!} = \frac{d^a}{dv^a} \Big[\log \varphi(e^v) \Big]_{v=0}.$$

Wir beweisen zunächst:

Satz 1. *Die Koeffizienten von* $\frac{v^a}{a!}$ *in der Entwicklung von* $\log\varphi(e^v)$ *bei* $v = 0$ *sind ganze Zahlen von* $R(\ell, w)$.

Beweis: Es ist, da wegen der gleichmäßigen Konvergenz gliedweise differenziert werden darf:

$$\begin{aligned}\frac{d\log\varphi(e^v)}{dv} &= \sum_{\nu=1}^{\infty}\frac{(-1)^{\nu-1}}{\nu}\nu\big(\varphi(e^v)-1\big)^{v-1}\varphi'(e^v)e^v;\ (\ell)\\ &= \left(\sum_{\nu=0}^{\infty}(-1)^{\nu}\big(\varphi(e^v)-1\big)^{\nu}\right)\cdot\varphi'(e^v)e^v;\ (\ell)\end{aligned}$$

Durch weitere Differentiation entstehen nur ganze rationale Ausdrücke aus φ und seinen Differentialquotienten. Nun haben die Differentialquotienten von φ nur Potenzen des Nenners $h(e^v)$ von φ zum Nenner, und $h(e^v)$ ist für alle $v \equiv 0 \bmod. \ell$, also speziell für $v = 0$ prim zu ℓ. Daher sind alle Differentialquotienten für $v = 0$ ganz für den Bereich von ℓ, also auch die Koeffizienten von $\frac{v}{1!}, \frac{v^2}{2!}, \dots$ in der Reihe für $\log\varphi(e^v)$. Das schließlich auch das absolute Glied ganz ist, ist trivial, weil es gleich III, 16

$$\log\varphi(1) \equiv 0 \bmod. \ell$$

ist, da $\varphi(1) \equiv 1 \bmod. \ell$.

Weiterhin gilt:

Satz 2. *Die Koeffizienten von* $\frac{v}{1!}, \dots, \frac{v^{\ell-2}}{(\ell-2)!}$ *in der Entwicklung von* $\log\varphi(e^v)$ *nach Potenzen von* v *sind mod.* ℓ *unabhängig von der speziellen Auswahl der Darstellung*

$$\alpha = \varphi(\zeta) = \frac{g(\zeta)}{h(\zeta)}$$

durch eine rationale Funktion φ, *für die Nenner* h (*und somit auch Zähler* g *wegen* $\alpha \equiv 1 \bmod. \mathfrak{l}$) *prim zu* $\mathfrak{l}$ *sind. Der Koeffizient von* $\frac{v^{\ell-1}}{(\ell-1)!}$ *ändert sich mod.* ℓ *um* $+\frac{\varphi(1)-\psi(1)}{\ell}$, *wenn* φ *durch* ψ *ersetzt wird.*

Beweis: Sei ψ eine zweite rationale Funktion obiger Eigenschaft, für die $\alpha = \psi(\zeta)$ wird. Dann ist

$$\frac{\psi(\zeta)}{\varphi(\zeta)} = 1,$$

also

$$\frac{\psi(e^v)}{\varphi(e^v)} = 1 + \chi(e^v) f(e^v),$$

wo

$$f(e^v) = 1 + e^v + \cdots + e^{(\ell-1)v},$$

und $\chi(e^v)$ eine solche rationale Funktion mit Koeffizienten aus $R(\ell, w)$ ist, deren Nenner (wegen der eindeutigen Zerlegbarkeit in Primfunktionen) höchstens das Produkt des Nenners von ψ mit dem Zähler von φ ist. Da beide nach Voraussetzung für φ und ψ (und wegen $\alpha \equiv 1 \mod. \mathfrak{l}$) für alle $v \equiv 0 \mod. \ell$ prim zu ℓ sind, sind $\chi(e^v)$ und alle seine Differentialquotienten für alle $v \equiv 0 \mod. \ell$ ganze Elemente aus $R(\ell, w)$. Weiter ist

III, 17

$$\log \psi(e^v) - \log \varphi(e^v) = \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} \big(\chi(e^v) f(e^v)\big)^{\nu} \ (\ell)$$

Wir haben dann nur zu zeigen, daß die Differentialquotienten der rechten Seite bis zum $(\ell-2)$–ten durch ℓ teilbar sind, wenn $v = 0$ gesetzt wird, und daß der $(\ell-1)$–te für $v = 0$ zu $\frac{\varphi(1)-\psi(1)}{\ell}$ mod. ℓ kongruent ist.

Nun ist zunächst

$$(1)\quad \frac{d}{dv} \log \psi(e^v) - \frac{d}{dv} \log \psi(e^v) = \sum_{\nu=1}^{\infty} (-1)^{\nu-1} \big(\psi(e^v) f(e^v)\big)^{\nu-1} \cdot \big(\chi' f + \chi f'\big) \cdot e^v,$$

also nach der obigen Bemerkung über χ alle Differentialquotienten für jedes $v \equiv 0 \mod. \ell$, speziell für $v = 0$ ganz.

Ferner ist

$$f(e^v) = \sum_{i=0}^{\ell-1} e^{iv} = \sum_{\mu=0}^{\infty} \frac{v^\mu}{\mu!} \sum_{i=0}^{\ell-1} i^\mu \equiv -\frac{v^{\ell-1}}{(\ell-1)!} + \sum_{\mu=\ell}^{\infty} \frac{v^\mu}{\mu!} \sum_{i=0}^{\ell-1} i^\mu \mod. \ell$$

wo die Kongruenz das Übereinstimmen entspr. Koeffizienten der Potenzen von v bedeutet; denn es ist ja

$$\sum_{i=0}^{\ell-1} i^\mu \equiv \begin{cases} 0 & \text{mod. } \ell, \text{ wenn } \mu = 0, 1, 2, \dots \ell-2 \\ -1 & \text{" " " } \mu = \ell - 1. \end{cases}$$

Daraus folgt durch Differentiation

$$f'(e^v) \cdot e^v \equiv -\frac{v^{\ell-2}}{(\ell-2)!} + \sum_{\mu=\ell-1}^{\infty} \frac{v^\mu}{\mu!} \sum_{i=0}^{\ell-1} i^{\mu+1} \text{ mod. } \ell.$$

Um daher in (1) die Koeffizienten von $1, \frac{v}{1!}, \ldots, \frac{v^{\ell-2}}{(\ell-2)!}$ zu finden, und zwar nur mod. ℓ, darf man an Stelle von $f(e^v)$ einfach 0 und an Stelle von $f'(e^v)e^v$ einfach $-\frac{v^{\ell-2}}{(\ell-2)!}$ setzen. Es kommt dann nur das Glied mit $\nu = 1$ für einen wirklichen Beitrag in Frage, und dieser Beitrag wird ersichtlich einfach III, 18

$$-\chi(1)\frac{v^{\ell-2}}{(\ell-2)!}$$

Daher folgt:

$$\begin{aligned} \frac{d^a}{dv^a} \log \psi(e^v)\Big|_0 &\equiv \frac{d^a}{dv^a} \log \varphi(e^v)\Big|_0 \text{ mod. } \ell \quad \text{für} \quad a = 1, \ldots \ell-2 \\ \frac{d^{\ell-1}}{dv^{\ell-1}} \log \psi(e^v)\Big|_0 &\equiv \frac{d^{\ell-1}}{dv^{\ell-1}} \log \varphi(e^v)\Big|_0 - \chi(1) \text{ mod. } \ell. \end{aligned}$$

Da schließlich

$$\frac{\psi(1)}{\varphi(1)} = 1 + \chi(1)f(1) = 1 + \ell\chi(1),$$

also

$$\chi(1) = \frac{\psi(1) - \varphi(1)}{\ell\varphi(1)}$$

ist, folgt wegen $\varphi(1) \equiv 1$ mod. ℓ, daß

$$\chi(1) \equiv \frac{\psi(1) - \varphi(1)}{\ell} \text{ mod. } \ell$$

ist, w. z. b. w.

Hiernach können wir jedem $\alpha \equiv 1$ mod. $\mathfrak{l}$ aus $K(\mathfrak{l})$ folgende eindeutig durch α bestimmten „*logarithmischen Differentialquotienten*“ zuordnen:

$$\begin{aligned} \ell_a(\alpha) &\equiv \frac{d^a}{dv^a} \log \varphi(e^v)\Big|_0 \text{ mod. } \ell \quad \text{für} \quad a = 1, \ldots \ell-2 \\ \ell_{\ell-1}(\alpha) &\equiv \frac{d^{\ell-1}}{dv^{\ell-1}} \log \varphi(e^v)\Big|_0 + \frac{\varphi(1)-1}{\ell} \text{ mod. } \ell, \end{aligned}$$

wenn $\alpha = \varphi(\zeta)$ in irgendeiner rationalen Darstellung durch ζ vorliegt, in der Zähler und Nenner prim zu $\mathfrak{l}$ sind.

III, 19

Satz 3. *Ist* $\alpha \equiv 1 \mod \mathfrak{l}^{\ell-1}$, *d. h.* mod. ℓ, *so ist*

$$\ell_a(\alpha) \equiv 0 \text{ mod. } \ell \quad \textit{für} \quad a = 1, 2, \ldots \ell - 2,$$

und wenn sogar $\alpha \equiv 1 \mod \mathfrak{l}^{\ell}$, *d. h.* mod $\ell\mathfrak{l}$ *ist, auch*

$$\ell_{\ell-1}(\alpha) \equiv 0 \text{ mod. } \ell.$$

Beweis: Es kann im ersten Falle

$$\alpha = 1 + \ell\chi(\zeta) \ (\mathfrak{l})$$

gesetzt werden, wo $\chi(\zeta)$ für den Beweis von $\mathfrak{l}$ ganz ist, also etwa als ganze rationale Funktion von ζ gewählt werden kann. Dann ist

$$\varphi(e^v) = 1 + \ell\chi(e^v)$$

und

$$\log\varphi(e^v) = \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} \ell^\nu \chi^\nu(e^v) \ (\ell)$$

$$\frac{d}{dv}\log\varphi(e^v) = \sum_{\nu=1}^{\infty} (-1)^{\nu-1} \ell^\nu \chi^{\nu-1}(e^v)\chi'(e^v)e^v \ (\ell)$$

Hierin sind alle Differentialquotienten der Glieder rechts durch ℓ teilbar, also für $v = 0$ speziell ebenfalls. Das gibt die Behauptung für den ersten Fall, da ja hier das Normierungsglied $\frac{\varphi(1)-1}{\ell}$ nicht in Betracht kommt. Ist ferner sogar $\alpha \equiv 1 \mod \mathfrak{l}^{\ell}$, so ist bei Benutzung obiger Darstellung für α

$$\chi(\zeta) \equiv 0 \text{ mod. } \mathfrak{l},$$
$$\chi(1) \equiv 0 \text{ mod. } \ell,$$

also

$$\frac{\varphi(1) - 1}{\ell} = \chi(1) \equiv 0 \text{ mod. } \ell,$$

sodaß auch $\ell_{\ell-1}(\alpha) \equiv 0$ mod. ℓ wird.

III, 20

Satz 4. *Es ist* $\ell_a(\alpha\beta) \equiv \ell_a(\alpha) + \ell_a(\beta)$ mod. ℓ *für irgendzwei* $\alpha, \beta \equiv 1$ mod. $\mathfrak{l}$ *und* $a = 1, 2, \ldots \ell - 1$.

Beweis: Ist $\varphi(e^v)$ eine α und $\psi(e^v)$ eine β zugeordnete Funktion, so kann $\varphi(e^v) \cdot \psi(e^v)$ als zugeordnete Funktion für $\alpha \cdot \beta$ verwendet werden. Es gilt dann

$$\log \varphi(e^v) + \log \psi(e^v) = \log \varphi(e^v) \cdot \psi(e^v) \ (\ell)$$

identisch in v. Also stimmen alle Differentialquotienten für $v = 0$ beider Seiten überein. Da auch

$$\frac{\varphi(1) - 1}{\ell} + \frac{\psi(1) - 1}{\ell} \equiv \frac{\varphi(1)\psi(1) - 1}{\ell} \quad \bmod \ell$$

für $\varphi(1) \equiv \psi(1) \equiv 1$ mod. ℓ gilt, folgt unmittelbar die Behauptung.

Satz 5. *Sind* $\alpha, \beta \equiv 1 \mod \mathfrak{l}$ *und*

$$\alpha \equiv \beta \mod \mathfrak{l}^{\ell-1},$$

so ist

$$\ell_a(\alpha) \equiv \ell_a(\beta) \mod \ell; \ (a = 1, 2, \dots \ell - 2)$$

Ist sogar $\alpha \equiv \beta \mod \mathfrak{l}^\ell$,
so ist auch

$$\ell_{\ell-1}(\alpha) \equiv \ell_{\ell-1}(\beta) \text{ mod. } \ell.$$

Beweis: Es ist $\frac{\alpha}{\beta} \equiv 1$ mod. $\mathfrak{l}^{\ell-1}$ bezw. mod. $\mathfrak{l}^\ell$. Hieraus folgt nach Satz 4 und 3 die Behauptung, wenn man noch (für die Division) die Bemerkung

$$\ell_a(1) \equiv 0 \text{ mod. } \ell; \ a = 1, 2, \dots \ell - 1$$

hinzufügt.

Satz 6. *Es ist für* $\alpha \equiv 1$ mod. $\mathfrak{l}$:

$$\ell_a(s\alpha) \equiv r^a \ell_a(\alpha) \text{ mod. } \ell$$

Beweis: Zu $s\alpha$ gehört die Funktion $\varphi(e^{rv})$. Entwickelt man $\varphi(e^{vr})$ nach Potenzen von vr, so entstehen die logarithmischen Differentialquotienten von α. Die von $s\alpha$ entstehen dann indem r abgespalten wird; also bekommt $\ell_a(\alpha)$ den Faktor r^a. Dies gilt auch für $a = \ell - 1$. Denn das Normierungsglied $\frac{\varphi(1)-1}{\ell}$ ist für α und $s\alpha$ dasselbe, und der Faktor ist $r^{\ell-1} \equiv 1$ mod. ℓ. III, 21

Satz 7. *Es sei* (w_i) *ein festes System von* f *linear unabhängigen Zahlen von* $R(\ell, w)$*, ferner, wie bei Takagi:*

$$g_a(s) = -r^a \frac{s^{\ell-1} - 1}{s - r^a},$$

wo s *und* r *die oben angegebene Bedeutung haben. Dann bilden die* $f(\ell - 1) + 1$ *Einseinheiten*

$$\kappa_{ai} = (1 + w_i \lambda^a)^{g_a(s)}; \quad 1 + \lambda^\ell = \kappa_0$$

ein Fundamentalsystem für die multiplikative Darstellung in $K(\mathfrak{l})$ *mit den Eigenschaften*

$$\kappa_{ai} \equiv 1 + w_i \lambda^a \mod \mathfrak{l}^{a+1}$$
$$\kappa_{ai}^{s-r^a} = 1 \ (\mathfrak{l})$$

Ist

$$\alpha = \prod_{a=1}^{\ell-1} \prod_{i=1}^{f} \kappa_{ai}^{c_{ai}} \kappa_0^{c_0} \alpha_0^\ell \ (\mathfrak{l})$$

die Darstellung einer Einseinheit durch jenes System, so gilt

$$\ell_a(\alpha) \equiv \left(\sum_{i=1}^{f} c_{ai} w_i \right) \cdot (-1)^a a! \text{ mod. } \ell$$

Beweis: Da $s\lambda^a \equiv r^a \lambda^a \mod \mathfrak{l}^{a+1}$ ist, und die w_i bei s invariant sind, ist

$$\kappa_{ai} \equiv 1 + g(r^a) w_i \lambda^a \equiv 1 + w_i \lambda^a \mod \mathfrak{l}^{a+1},$$

denn $g(r^a) \equiv 1$ mod. ℓ. Daher bilden die κ_{ai} mit κ_0 zusammen ein Fundamentalsystem für die Darstellung aller Einseinheiten von $K(\mathfrak{l})$. Daß $\kappa_{ai}^{s-r^a} = 1 \ (\mathfrak{l})$ ist, folgt aus

III, 22

$$g_a(s)(s - r^a) = s^{\ell-1} - 1 = 0.$$

Um schließlich die letzte Behauptung zu beweisen, ist nach Satz 4 und 3 nur noch

$$\ell_a(\kappa_{a'i}) \equiv \begin{cases} 0 \text{ mod. } \ell & \text{für} \quad a' \neq a \\ (-1)^a a! w_i \text{ mod. } \ell & \text{〃} \quad a' = a \end{cases}$$

zu zeigen.

Nun ist

$$\ell_a(\kappa_{a'i}) = \ell_a\left(1 + w_i\lambda^{a'}\right)^{g_{a'}(s)} = g_{a'}(r^a)\ell_a\left(1 + w_i\lambda^{a'}\right)$$

nach Satz 4 und 6. Da $g_{a'}(r^a) = 0$ für $a \neq a'$ folgt der erste Teil. Für $a = a'$ ist $g_a(r^a) \equiv 1 \mod. \ell$, also

$$\ell_a(\kappa_{ai}) \equiv \ell_a\left(1 + w_i\lambda^a\right) \mod. \ell.$$

Die $1 + w_i\lambda^a$ zugeordnete Funktion ist $1 + w_i\left(1 - e^v\right)^a = \varphi(e^v)$ und $\varphi(1) = 1$, sodaß für $a = \ell - 1$ kein Normierungsfaktor auftritt. Es ist

$$\begin{aligned} \log\varphi(e^v) &= \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} w_i^\nu \left(1 - e^v\right)^{a\nu} \\ &= \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} w_i^\nu \sum_{\mu=0}^{a\nu} (-1)^\mu \binom{a\nu}{\mu} e^{v\mu} \end{aligned}$$

Der a–te Diff. Quot. von $e^{v\mu}$ bei $v = 0$ ist μ^a, also

$$\ell_a(\kappa_{ai}) = \sum_{\nu=1}^{\infty} \frac{(-1)^{\nu-1}}{\nu} w_i^\nu \sum_{\mu=0}^{a\nu} (-1)^\mu \binom{a\nu}{\mu} \mu^a.$$

Nun ist die $\sum\limits_{\mu}$ die $a\nu$–te Differenz von $0^a, 1^a, 2^a, \ldots$ also für $\nu > 1$ sicher Null, nur für $\nu = 1$ gleich $(-1)^a a!$, daher

$$\ell_a(\kappa_{ai}) \equiv (-1)^a a! w_i \mod. \ell, \quad \text{w. z. b. w.}$$

III, 23

Es seien nun im folgenden alle zu betrachtenden Zahlen aus dem *absoluten* Körper K gewählt, und zwar so, daß sie neben der (als Kongruenzen nach genügend hohen Moduln aufzufassenden) Bedingungen in $K(\mathfrak{l})$, die wir näher angeben, für alle von $\mathfrak{l}$ verschiedenen Primteiler von ℓ in K der Bedingung genügen, daß sie nach genügend hohen Potenzen $\equiv 1$ sind. Dann gilt für zwei (zueinander kernprime*)) zu ℓ prime solche Zahlen α, β:

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \left(\frac{\alpha, \beta}{\mathfrak{l}}\right)^{-1} \quad \text{kurz } = (\alpha, \beta)$$

*) Bei den Umkehrsymbolen sollen ferner die beiden Komponenten durch geeignete Wahl in genügend hoch festgelegten Restklassen mod $\mathfrak{l}^N$ kernprim zu einander sein.

Mit dem genannten Sinne gilt dann:

Satz 8. *Es ist stets:*

$$\begin{aligned} (\kappa_{ai}, \kappa_0) &= 1 \\ (\kappa_{ai}, \kappa_{bj}) &= 1 \quad \text{wenn} \quad a+b \neq \ell \end{aligned}$$

Beweis: Die erste Beziehung habe ich in Z. V. bewiesen. Die zweite folgt, wie bei Takagi so:

$$s(\kappa_{ai}, \kappa_{bj}) = (\kappa_{ai}, \kappa_{bj})^r, \quad \text{weil der Wert eine Potenz von } \zeta \text{ ist.}$$
$$s(\kappa_{ai}, \kappa_{bj}) = (s\kappa_{ai}, s\kappa_{bj}) = (\kappa_{ai}, \kappa_{bj})^{r^{a+b}}, \quad \text{weil } \mathfrak{l} \text{ bei } s \text{ invariant und}$$

nach Satz 7. Da

$$r^{a+b} \not\equiv r \text{ mod. } \ell \quad \text{für} \quad a+b \neq \ell,$$

III, 24 (im Def. Bereich der a, b), folgt die zweite Behauptung. In dem a. S. 23] oben genannten Sinne gilt

Satz 9. *Für* $\alpha, \beta \equiv 1 \mod \mathfrak{l}$ *ist*

$$(\alpha, \beta) = \zeta^{\sum_{a=1}^{\ell-1} C_a S_w \left(\ell_a(\alpha) \cdot \ell_{\ell-a}(\beta)\right)}$$

wo S_w *die Spur in* $R(\ell, w)$ *bezeichnet, und die* C_a *nur von* a *abhängige rationale ganze Zahlen sind.*

Beweis: Sei

$$\begin{aligned} \alpha &= \prod_{a=1}^{\ell-1} \prod_{i=1}^{f} \kappa_{ai}^{c_{ai}} \kappa_0^{c_0} \alpha_0^{\ell} \; (\mathfrak{l}) \\ \beta &= \prod_{b=1}^{\ell-1} \prod_{j=1}^{f} \kappa_{bj}^{d_{bj}} \kappa_0^{d_0} \beta_0^{\ell} \; (\mathfrak{l}) \end{aligned}$$

und seien die Faktoren mit gleichem a bezw. b in α_a, β_b zusammengefaßt, sodaß

$$\begin{aligned} \alpha &= \alpha_1 \ldots \alpha_{\ell-1} \kappa_0^{c_0} \alpha_0^{\ell} \; (\mathfrak{l}) \\ \beta &= \beta_1 \ldots \beta_{\ell-1} \kappa_0^{d_0} \beta_0^{\ell} \; (\mathfrak{l}) \end{aligned}$$

mit

$$\alpha_a = \prod_{i=1}^{f} \kappa_{ai}^{c_{ai}} \ (\mathfrak{l})$$
$$\beta_b = \prod_{j=1}^{f} \kappa_{bj}^{d_{bj}} \ (\mathfrak{l})$$

geschrieben wird. Dann ist nach Satz 8:

$$(\alpha, \beta) = (\alpha_1, \beta_{\ell-1})(\alpha_2, \beta_{\ell-2}) \cdots (\alpha_{\ell-1}, \beta_1)$$

Nun ist nach meiner Arbeit Rez. Ges.*)

$$(\alpha_a, \beta_{\ell-a}) = \zeta^{C'_a S_w\left(\frac{\alpha_a - 1}{\lambda^a} \frac{\beta_{\ell-a}-1}{\lambda^{\ell-a}}\right)}$$

mit einem festen, also nur von a abhängigen, ganzen rationalen C'_a. Da nun III, 25

$$\frac{\alpha_a - 1}{\lambda^a} \equiv \sum_{i=1}^{f} c_{ai} w_i \, ; \; \frac{\beta_{\ell-a} - 1}{\lambda^{\ell-a}} \equiv \sum_{j=1}^{f} d_{\ell-a,j} w_j \mod. \mathfrak{l}$$

ist, folgt nach Satz 7

$$(\alpha_a, \beta_{\ell-a}) = \zeta^{C'_a S_w\left(\frac{\ell_a(\alpha)}{(-1)^a a!} \frac{\ell_{\ell-a}(\beta)}{(-1)^{\ell-a}(\ell-a)!}\right)}, \quad \text{w. z. b. w.}$$

Um noch den Zusammenhang zwischen den C'_a und der C_0 des Satzes zu finden, ist die Relation

$$C'_a \equiv -a!(\ell - a)! C_a \mod. \ell$$

umzuformen. Nun ist

$$\binom{\ell}{a} = \frac{\ell!}{a!(\ell-a)!}\, ; \quad \text{also} \quad \frac{1}{\ell}\binom{\ell}{a} \equiv \frac{-1}{a!(\ell-a)!} \mod. \ell,$$

und somit

$$C_a \equiv \frac{1}{\ell}\binom{\ell}{a} C'_a \mod \ell.$$

*) S_w von Zahlen in $K(\mathfrak{l})$ bedeutet, daß die Spur in $R(\ell, w)$ ihrer Kongruenzwerte mod. $\mathfrak{l}$ zu nehmen ist.

Ferner ist

$$\frac{1}{\ell}\binom{\ell}{a} = \frac{(\ell-1)(\ell-2)\dots\big(\ell-(a-1)\big)}{a!} \equiv$$
$$\equiv \frac{(-1)^{a-1}(a-1)!}{a!} \equiv \frac{(-1)^{a-1}}{a} \mod. \ell.$$

Somit gilt:

Satz 10. *Es ist $C'_a \equiv (-1)^{a-1} a C_a \mod. \ell$, wo C_a durch Satz 9 und C'_a durch die Formel a. v. S.] unten definiert ist.*

Weiter beweisen wir:

Satz 11. *Es ist $C'_a \equiv -a \mod. \ell$, also $C_a \equiv (-1)^a \mod \ell$.*

Beweis: Sei

$$\alpha_a = 1 + g\lambda^a + \cdots \quad \text{in } k_\zeta; \quad g \not\equiv 0 \mod. \ell$$
$$\beta_{\ell-a} = 1 + u\lambda^{\ell-a} + \cdots \quad \text{in } K; \quad S_w(u) \not\equiv 0 \mod. \ell$$

III, 26 Dann ist nach Hilfssatz 2 meiner Arbeit über die log. Diff. Quot.

$$(\alpha_a, \beta_{\ell-a})_K = \big(\alpha_a, n(\beta_{\ell-a})\big)_{k_\zeta},$$

wo n die Relativnorm nach k_ζ ist und der angehängte Index den Körper bezeichnet, auf den sich die Symbole beziehen.

Nun ist einerseits nach S. 24] unten

$$(\alpha_a, \beta_{\ell-a})_K = \zeta^{C'_a S_w(gu)} = \zeta^{C'_a g S_w(u)}.$$

Andererseits, etwa nach der Takagischen Arbeit mit Takagis κ_a im Kreiskörper:

$$\big(\alpha_a, n(\beta_{\ell-a})\big)_{k_\zeta} = \big(1 + g\lambda^a + \cdots, 1 + S_w(u)\lambda^{\ell-u} + \cdots\big)_{k_\zeta}$$
$$= \Big(\kappa_a^{-g}, \kappa_{\ell-a}^{-S_w(u)}\Big)_{k_\zeta} = \zeta^{-agS_w(u)}$$

Wegen $gS_w(u) \not\equiv 0 \mod. \ell$ ist also $C'_a \equiv -a \mod. \ell$, w. z. b. w.

Damit wird jetzt Satz 9 zu:

Satz 12. *Für* $\alpha, \beta \equiv 1 \mod \mathfrak{l}$ *(unter den a. S. 23] oben genannten anderen Bedingungen) ist*

$$(\alpha, \beta) = \zeta^{\sum_{a=1}^{\ell-1} (-1)^a S_w \left(\ell_a(\alpha)\ell_{\ell-a}(\beta)\right)}.$$

Hierin kann nötigenfalls, mit Vorzeichenumkehrung, die S_w *durch die* $S_{\mathfrak{l}}$*, d. h. die Spur in* $K(\mathfrak{l})$ *ersetzt werden, da allgemein*

$$S_{\mathfrak{l}}(u) \equiv -S_w(u) \text{ mod. } \ell,$$

wenn u *in* $R(\ell, w)$.

3.6 Normierung des Hilbertschen Normenrestsymbols. (31.5.1924)

Hilbert's definition of the (global) norm residue symbol was defined via power residue symbols. Hasse constantly tried, partially in collaboration with Hensel, to give a more conceptual definition of the norm residue symbol, based on local considerations. The main problem is the local definition of a normalization such that Hilbert's product formula holds. Hasse notes here that this can be achieved in the field of ℓ-th roots of unity. In his paper [Has25d] *he extends this to more general fields. But for arbitrary fields this will be achieved later only, after local class field theory had been established* [Has33a].

III, 27

31. V. 24.

In meiner Arbeit N. R. II. [1] zeigte ich, daß das Symbol $\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)$ für alle α, β aus $k(\mathfrak{l})$ bis auf die einmalige Auswahl der zugrundegelegten primitiven Einheitswurzel ζ eindeutig bestimmt ist.

Eine weitere Normierung kann natürlich nur den Sinn haben, relativ zu einem fest vorgegebenen ζ die Definition jener Symbole zu geben, sodaß nachher bei festem ζ Symbole für verschiedene $\mathfrak{l}$ nebeneinander betrachtet werden können.

Jene Normierung wird auf Grund des Hilbertschen Reziprozitätsgesetzes geliefert, indem

$$\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)^{-1} = \prod_{\mathfrak{p}} \left(\frac{\overline{\alpha},\beta}{\mathfrak{p}}\right) \qquad \text{über alle zu } \ell \text{ primen } \mathfrak{p}$$

gesetzt wird, wo $\overline{\alpha}$ für den Bereich von $\mathfrak{l}$ hinreichend nahe an α liegt, für die Bereiche der übrigen Primteiler von $\mathfrak{l}$ jedoch hinreichend nahe an 1, und $\overline{\alpha}, \beta$ in k sind.

Nach dieser Normierung haben bei fest vorgegebenem ζ die Symbole $\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)$ auch für beliebige α, β aus $k(\mathfrak{l})$ einen eindeutigen Sinn, da solche α, β beliebig nahe durch Zahlen aus k approximiert werden können. Für α, β aus k gilt nach jener Normierung

$$\prod_{\mathfrak{p}} \left(\frac{\alpha,\beta}{\mathfrak{l}}\right) = 1 \qquad \text{erstreckt über alle } \mathfrak{p}.$$

III, 28

Für den Fall, daß $\mathfrak{l}$ eine zu ℓ prime Ordnung e hat, läßt sich nach den Ergeb-

[1] Es handelt sich um [Has24b].

nissen meiner Arbeit über das Reziprozitätsgesetz (Crelle 153, S. 195 ff) [2] jene Normierung auch *allein vom Bereich* $k(\mathfrak{l})$ aus angeben, und zwar so:

Man wähle ein Fundamentalsystem:

$$\lambda = \eta_0\,;\ \eta_1, \ldots, \eta_m\,;\ \eta_a = \eta_{m+1} \quad (m = ef)$$

für die multiplikative Darstellung in $k(\mathfrak{l})$ und bestimme eine Bilinearform $L(x|y)$, sodaß für

$$\begin{aligned} \alpha &= \prod \eta_i^{x_i} \alpha_0^\ell \ (\mathfrak{l}) \\ \beta &= \prod \eta_\kappa^{y_\kappa} \beta_0^\ell \ (\mathfrak{l}) \end{aligned}$$

gilt:

$$L(x|y) \equiv 0 \ \text{mod.}\ \ell \ \textit{dann und nur dann, wenn}\ \left(\tfrac{\alpha,\beta}{\mathfrak{l}}\right) = 1.$$

Diese Bilinearform ist bis auf einen konstanten, zu ℓ primen Faktor mod. ℓ eindeutig bestimmt. Man normiere nun $L(x|y)$ so, daß der für

$$\begin{aligned} \alpha &= 1 + u\ell\,; \quad s_{\mathfrak{l}}(u) = u + u^\ell + \cdots + u^{\ell^{f-1}} \not\equiv 0 \ \text{mod.}\ \ell \\ \beta &= \zeta \end{aligned}$$

resultierende Wert

$$L(x_0|y_0) \equiv e s_{\mathfrak{l}}(u) \ \text{mod.}\ \ell$$

wird.

Dies ist wegen $\left(\frac{1+u\ell,\zeta}{\mathfrak{l}}\right) \neq 1$ und $e \not\equiv 0$ mod. ℓ möglich. Dann ist die hierdurch implizierte Normierung der $\left(\frac{\alpha,\beta}{\mathfrak{l}}\right)$ identisch mit der Hilbertschen.

[2] Es handelt sich um [Has24a].

3.7 Der zweite Ergänzungssatz in gewissen Oberkörpern des Kreiskörpers. (5.6.1924)

The second supplementary law of the ℓ-th power reciprocity law deals with power residue symbols of the form $\left(\frac{\lambda}{\mathfrak{p}}\right)$ for $\lambda = 1 - \zeta$. Here Hasse considers more generally symbols $\left(\frac{\Lambda}{P}\right)$ for elements Λ of an extension of $\mathbb{Q}(\zeta)$ divisible by primes above ℓ. This is preparatory work for Hasse's paper [Has25b].

III, 29

5. VI. 24.

Ich gehe aus von der in meiner Arbeit R. G. III erhaltenen Formel

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\sum_{i=1}^{n} S_i\left\{\sum_{\kappa=1}^{\ell-1} \kappa \frac{s_i(\zeta^{-\kappa}\log\alpha)}{\ell}\cdot\frac{s_i(\zeta^{\kappa}\log\beta)}{\ell} + s_i\left(\frac{\alpha-1}{\lambda}\right)^{\ell}\frac{s_i(\log\beta)}{\ell} - s_i\left(\frac{\beta-1}{\lambda}\right)^{\ell}\frac{s_i(\log\alpha)}{\ell}\right\}}$$

Dabei ist ℓ eine ungerade Primzahl, k ein solcher Oberkörper von k_ζ, daß

$$\mathfrak{l} = (\lambda) = (1-\zeta) = \mathfrak{l}_1\mathfrak{l}_2\dots\mathfrak{l}_n\,; \quad (\mathfrak{l}_i \text{ vom Grade } f_i)$$

in k gilt. S_i, s_i sind:

s_i = Spur von $k_{\mathfrak{l}_i}$ nach Koeffizientenkörper $R_\ell(w_i)$
S_i = 〃 〃 $R_\ell(w_i)$ nach rat. ℓ–adischen Körper R_ℓ.

α und β befriedigen die Bedingung $\alpha, \beta \equiv 1 \mod. \mathfrak{l}$
Es werde die Funktion im Exponenten so bezeichnet

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \zeta^{\sum_{i=1}^{n}\varphi_i(\alpha,\beta)},$$

sodaß

$$\left(\frac{\alpha,\beta}{\mathfrak{l}_i}\right)^{-1} = \zeta^{\varphi_i(\alpha,\beta)}$$

ist.

Der zweite Ergänzungssatz stellt die Aufgabe, für ein beliebiges, durch Primteiler $\mathfrak{l}_i$ teilbares

$$\Lambda \sim \mathfrak{l}_1^{a_1}\dots\mathfrak{l}_n^{a_n}\mathfrak{a}$$

Aussagen über $\left(\frac{\Lambda}{\alpha}\right)$ zu machen. Ohne Beschränkung darf

$$\alpha \equiv 1 \mod \mathfrak{l}$$

angenommen werden, da sonst $\alpha^{\ell^{f_1 \cdots f_n}-1}$ dies leistet.

Es sei nun α außerdem so beschaffen, daß $\mathfrak{a}$ kernprim zu α ist. Dann gilt: III, 30

$$\prod_{\mathfrak{p}} \left(\frac{\Lambda, \alpha}{\mathfrak{p}}\right) = \left(\frac{\Lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{a}}\right)^{-1} = \prod_i \left(\frac{\Lambda, \alpha}{\mathfrak{l}_i}\right)^{-1}.$$

Um $\left(\frac{\Lambda,\alpha}{\mathfrak{l}_i}\right)^{-1}$ zu bestimmen, zerlegen wir

$$\left(\frac{\Lambda, \alpha}{\mathfrak{l}_i}\right)^{-1} = \left(\frac{\Lambda\lambda^{-a_i}, \alpha}{\mathfrak{l}_i}\right)^{-1} \cdot \left(\frac{\lambda, \alpha}{\mathfrak{l}_i}\right)^{-a_i}$$

Wir bestimmen zunächst $\left(\frac{\lambda,\alpha}{\mathfrak{l}_i}\right)^{-1}$. Nach einer früheren Arbeit von Artin und mir ist für $\alpha \equiv 1$ mod. $\mathfrak{l}$

$$\left(\frac{\lambda}{\alpha}\right) = \prod \left(\frac{\lambda, \alpha}{\mathfrak{l}_i}\right)^{-1} = \zeta^{-S\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)} = \zeta^{-\sum_{i=1}^n S_{\mathfrak{l}_i}\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)}$$

wo $S_{\mathfrak{l}_i}$ die Spur $S_i s_i$ in $k_{\mathfrak{l}_i}$ bezeichnet. Wenn nun α für alle von $\mathfrak{l}_i$ verschiedenen $\mathfrak{l}_\kappa$ eine ℓ–te Potenz ist, folgt

$$\prod \left(\frac{\lambda, \alpha}{\mathfrak{l}_\kappa}\right)^{-1} = \left(\frac{\lambda, \alpha}{\mathfrak{l}_i}\right)^{-1} = \zeta^{-\sum_{\kappa=1}^n S_{\mathfrak{l}_\kappa}\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)} = \zeta^{-S_{\mathfrak{l}_i}\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)},$$

da dann für die $\mathfrak{l}_\kappa$

$$\log \alpha \equiv 0 \text{ mod. } \mathfrak{l}_\kappa^{\ell+1}$$

ist. Daher gilt allgemein in $k_{\mathfrak{l}_i}$ für $\alpha \equiv 1 \mod \mathfrak{l}_i$:

$$\left(\frac{\lambda, \alpha}{\mathfrak{l}_i}\right)^{-1} = \zeta^{-S_{\mathfrak{l}_i}\left(\frac{\zeta \log \alpha}{\ell\lambda}\right)}.$$

Denn jedes solche α aus $k_{\mathfrak{l}_i}$ kann durch ein den obigen Bedingungen entsprechendes α aus k so ersetzt werden, daß der multiplikative Unterschied nur eine ℓ–te Potenz in $k_{\mathfrak{l}_i}$ ist, für die das linksstehende Symbol wegfällt und ebenso der rechtsstehende Exponent.

Ferner ist $\left(\frac{\Lambda\lambda^{-a_i},\alpha}{\mathfrak{l}_i}\right)^{-1}$ zu bestimmen. $\Lambda\lambda^{-a_i}$ ist prim zu $\mathfrak{l}_i$. Seine $\left(\ell^{f_i}-1\right)$–te Potenz ist also $\equiv 1 \mod. \mathfrak{l}_i$ und

$$\left(\frac{\Lambda\lambda^{-a_i},\alpha}{\mathfrak{l}_i}\right)^{-1} = \left(\frac{(\Lambda\lambda^{-a_i})^{\ell^{f_i}-1},\alpha}{\mathfrak{l}_i}\right)$$

Daher wird

$$\left(\frac{\Lambda\lambda^{-a_i},\alpha}{\mathfrak{l}_i}\right)^{-1} = \zeta^{-\varphi_i\left(\left(\frac{\Lambda}{\lambda^{a_i}}\right)^{\ell^{f_i}-1},\alpha\right)}.$$

III, 31 Hieraus folgt nun durch Zusammensetzung die Formel

$$\boxed{\left(\frac{\Lambda}{\alpha}\right)\left(\frac{\alpha}{\mathfrak{a}}\right)^{-1} = \zeta^{-\sum_{i=1}^{n}\varphi_i\left[\left(\frac{\Lambda}{\lambda^{a_i}}\right)^{\ell^{f_i}-1},\alpha\right]-\sum_{i=1}^{n}a_i S_{\mathfrak{l}_i}\left(\frac{\zeta\log\alpha}{\ell\lambda}\right)}}$$

Diese gilt unter folgenden Voraussetzungen:

1.) k Oberkörper von k_ζ in dem der Primteiler $\mathfrak{l}=(\lambda)$ von k_ζ so zerfällt

$$\mathfrak{l} = \mathfrak{l}_1\ldots\mathfrak{l}_n\,; \quad (\mathfrak{l}_i \text{ vom Grade } f_i)$$

2.) $\alpha\equiv 1 \mod. \mathfrak{l}$

3.) $(\Lambda) = \mathfrak{l}_1^{a_1}\ldots\mathfrak{l}_n^{a_n}\mathfrak{a}\,; \quad (\mathfrak{a},\ell)=1$

4.) $\mathfrak{a}$ kernprim zu α.

3.8 Darstellung endlicher Gruppen durch Matrizen. (Juni 1924)

Matrix representation theory of finite groups. This entry and some of the later entries document Hasse's interest in the representations of (finite) groups by matrices. This appears motivated by his contact with Artin who was interested in the proof of his reciprocity law which came up in connection with Artin's new L-functions belonging to characters of representations of the Galois group.

III, 32

Juni 1924

Sei $\mathfrak{G}$ eine endliche Gruppe der Ordnung g, deren Elemente mit $E, R, S, T, P, Q, \ldots$ bezeichnet werden.

Ferner sei k ein beliebiger Körper der Charakteristik 0. Dann suchen wir Darstellungen von $\mathfrak{G}$ durch Matrizen aus k, die wir mit $A_R, A_S, \ldots, B_R, \ldots$ bezeichnen. Wir setzen die Determinanten der Matrizen $\neq 0$ voraus.

Satz 1. *Ist $\Gamma = \{A_R\}$ eine Darstellung von $\mathfrak{G}$ durch Matrizen in k, so ist auch $\overline{\Gamma} = \left\{{A'_R}^{-1}\right\} = \{\overline{A}_R\}$ eine solche vom selben Grad und $\overline{\overline{\Gamma}} = \Gamma$; (die adjungierte Darstellung zu Γ).*

Beweis: Klar.

Zwei Darstellungen Γ, Δ heißen *äquivalent in k*, wenn eine Matrix C nicht verschwindender Determinante in k existiert, sodaß

$$C^{-1}\Gamma C = \Delta$$

ist, d. h. diese Gleichung für alle entsprechenden Matrizen aus Γ und Δ gilt.

Die Darstellung Γ heißt *irreduzibel in k*, wenn sie keiner solchen Darstellung in k äquivalent ist, deren Matrizen sämtlich in ein– u. derselben Weise in Partialsysteme zerfallen. Jede Darstellung läßt sich dann in k in eine solche transformieren, die in eine *Summe* irreduzibler Bestandteile zerfällt:

$$\Gamma \sim n_1\Gamma_1 + n_2\Gamma_2 + \cdots + n_r\Gamma_r$$

Ob dies auf *nur eine* Weise möglich ist, bleibt fürs erste dahingestellt.

Satz 2. *Mit Γ ist auch $\overline{\Gamma}$ irreduzibel oder reduzibel in k.*

Beweis: Aus $C^{-1}\Gamma C = \Delta$ folgt $\overline{C}^{-1}\overline{\Gamma}\,\overline{C} = \overline{\Delta}$ und umgekehrt.

III, 33

Die Summe der Diagonalglieder einer Matrix A heißt ihr *Charakter* $\chi(A)$, die Funktion

$$\chi_\Gamma(R) = \chi_\Gamma(A_R)$$

der Gruppenelemente R, die aus einer Darstellung Γ entspringt, heißt der *Charakter* von Γ. Der Charakter von Γ besteht aus g Elementen von k. Es gilt

Satz 3. *Der Charakter von* Γ *ist invariant gegen Transformation in* k, (*sogar gegen Transformation in beliebigen Oberkörpern von* k).

Beweis: Der Beweis beruht auf der rein algebraischen Identität

$$\chi(A) = \chi(C^{-1}AC)$$

für eine beliebige Matrix A und eine beliebige Matrix C nicht verschwindender Determinante.

Satz 4. *Ist* $\Gamma \sim n_1\Gamma_1 + \cdots + n_r\Gamma_r$, *so ist*

$$\chi_\Gamma(R) = n_1\chi_{\Gamma_1}(R) + \cdots + n_r\chi_{\Gamma_r}(R).$$

Beweis: Klar.

Satz 5. *Ist* Γ *eine Darstellung der speziellen Form:*

$$A_R = \begin{pmatrix} B_R & 0 \\ D_R & C_R \end{pmatrix}$$

(*halbreduzible Darstellung*), *so bilden die Matrizen* B_R, C_R *selbst Darstellungen, während die* D_R *sich gemäß*

$$D_{RS} = D_R B_S + C_R D_S$$

komponieren.

Beweis: Klar.

Satz 6. *Jede halbreduzible Darstellung in* k *ist reduzibel in* k, *nämlich*

$$A_R = \begin{pmatrix} B_R & 0 \\ D_R & C_R \end{pmatrix} \sim \begin{pmatrix} B_R & 0 \\ 0 & C_R \end{pmatrix}.$$

Beweis: Wir setzen

$$F = \frac{1}{g}\sum_S D_S B_{S^{-1}}$$

und

$$C = \begin{pmatrix} E & 0 \\ F & E \end{pmatrix}.$$

F und C sind Matrizen aus k. Es ist für jedes R: III, 34

$$C^{-1}A_R C = \begin{pmatrix} E & 0 \\ -F & E \end{pmatrix} \begin{pmatrix} B_R & 0 \\ D_R & C_R \end{pmatrix} \begin{pmatrix} E & 0 \\ F & E \end{pmatrix} = \begin{pmatrix} B_R & 0 \\ D_R + C_R F - F B_R & C_R \end{pmatrix}$$

und

$$\begin{aligned} D_R + C_R F - F B_R &= D_R + \frac{1}{g}\sum_S C_R D_S B_{S^{-1}} - \frac{1}{g}\sum_S D_S B_{S^{-1}} B_R \\ &= D_R + \frac{1}{g}\sum_S D_{RS} B_{S^{-1}} - \frac{1}{g}\sum_S D_R B_S B_{S^{-1}} - \frac{1}{g}\sum_S D_S B_{S^{-1}R} \end{aligned}$$

Nimmt man nun den sogleich zu erbringenden Nachweis hinzu, daß

$$B_S B_{S^{-1}} = B_{SS^{-1}} = B_E = E$$

sein muß, so wird

$$\frac{1}{g}\sum_S D_R B_S B_{S^{-1}} = D_R.$$

Ferner ist

$$\sum_S D_{RS} B_{S^{-1}} = \sum_S D_S B_{S^{-1}R},$$

woraus

$$D_R + C_R F - F B_R = 0$$

folgt, w. z. b. w.

Satz 7. *Zu jeder Darstellung in k ist*

$$A_E = E$$

die Einheitsmatrix, also auch $A_{S^{-1}} = A_S^{-1}$.

Beweis: Die Matrix A_E muß der Bedingung genügen

$$A_E A_E = A_{EE} = A_E.$$

Nennt man ihre Koeffizienten e_{ik}, so muß also gelten:

$$\sum_{\nu=1}^{n} e_{i\nu} e_{\nu\kappa} = e_{i\kappa}\,; \quad (i,\kappa = 1,2,\ldots,n)$$

Für festes κ sind das n inhomogene Gleichungen für die n „Variablen" $e_{1\kappa},\ldots,e_{n\kappa}$ mit der Matrix A_E, für die $|A_E| \neq 0$. Sie haben also eine und nur eine Lösung, und diese ist ersichtlich

$$e_{\kappa\kappa} = 1, \quad e_{i\kappa} = 0; \quad i \neq \kappa.$$

Da das für jedes $\kappa = 1,2,\ldots,n$ gilt, ist A_E die Einheitsmatrix.

Satz 8. *Sind Γ, Δ zwei irreduzible Darstellungen in k der Grade n, m, so folgt aus dem Bestehen der Identität*

$$\Gamma' F \Delta = F$$

für irgendeine rechteckige Matrix F aus k vom Typus $n \cdot m$, daß entweder

$$F = 0$$

oder $n = m$ und

$$|F| \neq 0,$$

sodaß dann

$$\overline{\Gamma} \sim \Delta \quad \textit{und} \quad \Gamma \sim \overline{\Delta}$$

ist.

III, 35 *Beweis*: Bekanntlich lassen sich zu F, falls $F \neq 0$ ist, zwei Matrizen C, D aus k von nicht verschwindender Determinante angeben, sodaß

$$C' F D = E_r$$

die r–reihige Einheitsmatrix ist. Dabei ist C vom Typus $n \cdot n$, D vom Typus $m \cdot m$, und r ist der Rang von F.

Es ist dann auch

$$(C'\Gamma'C'^{-1})\,(C'FD)\,(D^{-1}\Delta D) = C'FD = E_r$$

d. h.

$$\left(C^{-1}\Gamma C\right)' E_r \left(D^{-1}\Delta D\right) = E_r$$

Es ist also keine Beschränkung, wenn wir Γ, Δ von vorneherein so durch in k äquivalente Darstellungen ersetzt haben, daß $F = E_r$ ist. Dann gilt also für jedes A_R aus Γ und B_R aus Δ:

$$A'_R E_r B_R = E_r, \quad \text{d. h.} \quad E_r B_R = \overline{A}_R E_r$$

Ist hierin nun $r < n$ oder $r < m$, so folgt in bekannter Weise die Koeffizientenvergleichung die Halbreduzibilität von Γ oder Δ, also nach Satz 6 die Reduzibilität von Γ oder Δ, was mit der Voraussetzung in Widerspruch. Also ist $r = n = m$ und $\Delta \sim \overline{\Gamma}$, w. z. b. w.

Satz 9. *ist k algebraisch abgeschlossen und Γ irreduzibel in k, ferner F eine solche Matrix aus k, daß identisch $F\Gamma = \Gamma F$ ist, so ist $F = aE$, so a Zahl aus k ist.* III, 36

Beweis: Nach Voraussetzung über k hat die algebraische Gleichung

$$|F - aE| = 0$$

in k eine Lösung a. Aus der Voraussetzung über Γ folgt für die Matrix $F - aE$ dann die Identität

$$\begin{aligned} \Gamma^{-1}(F-aE)\Gamma &= F - aE \\ \text{d. h.} \quad \overline{\Gamma}'(F-aE)\Gamma &= F - aE \end{aligned}$$

Nach Satz 8 folgt dann aus der Irreduzibilität von Γ in k, daß

$$F - aE = 0$$

sein muß, w. z. b. w.

Satz 10. *Ist $\mathfrak{G}$ eine Abelsche Gruppe, m das kleinste Vielfache der Ordnungen ihrer Elemente, und enthält k die m–ten Einheitswurzeln, so sind die irreduziblen Darstellungen von Γ vom Grade 1, also Einheitswurzelgruppen.*

Beweis: Ist Γ eine in k irreduzible Darstellung und A_P eines ihrer Elemente, so gilt identisch

$$A_P\Gamma = \Gamma A_P.$$

Nun sind die m–ten Potenzen der Wurzeln von

$$|A_P - xE| = 0$$

die Wurzeln von

$$|A_P^m - yE| = 0$$

also wegen $A_P^m = A_E = E$ sämtlich gleich 1, d. h. die Wurzeln der ersteren Gleichung sämtlich m–te Einheitswurzeln, die nach Annahme in k liegen. Aus dem Beweis zu Satz 9 folgt also, daß

$$A_P = \varrho E$$

ist, wo ϱ eine m–te Einheitswurzel ist. Die Matrizen A_P von Γ müssen also den Grad 1 haben, da sonst Γ reduzibel wäre.

III, 37

Satz 11. *Sind $\Gamma = (A_R) = (a_{i\kappa}^R)$ und $\Delta = (B_R) = (b_{i\kappa}^R)$ zwei in k irreduzible Darstellungen und $\Delta \not\sim \overline{\Gamma}$, so gelten für die inneren Produkte der Stellenzeilen von Γ und Δ die Relationen*

$$\sum_R a_{i\kappa}^R b_{\mu\nu}^R = 0.$$

Ist ferner k algebraisch abgeschlossen und Γ irreduzibel in k, $\overline{\Gamma} = (\overline{A}_R) = (\overline{a}_{i\kappa}^R)$ die adjungierte Darstellung, so gilt

$$\sum_R a_{i\kappa}^R \overline{a}_{\mu\nu}^R = \begin{cases} 0, & \text{wenn} \quad (i,\kappa) \neq (\mu,\nu) \\ \frac{g}{f}, & \quad " \quad (i,\kappa) = (\mu,\nu). \end{cases}$$

Dabei ist f der Grad von Γ.

Beweis: Sei $C = (c_{\mu\nu})$ eine beliebige Matrix aus k und

$$D = \sum_R A'_R C B_R$$

Dann ist

$$A'_P D B_P = \sum_R A'_{RP} C B_{RP} = D.$$

Die Matrix D erfüllt also die Voraussetzungen von Satz 8, sodaß wegen $\overline{\Gamma} \not\sim \Delta$ folgt:

$$D = \sum_R A'_R C B_R = 0,$$

was auch C sei. Nun ist

$$D = \sum_R A'_R C B_R = \left(\sum_R \sum_{\mu,\nu} a^R_{\mu i} c_{\mu\nu} b^R_{\nu\kappa} \right)$$

Setzt man alle $c_{\mu\nu}$ bis auf eins gleich Null, dies eine aber etwa gleich 1, so folgt

$$\sum_R a^R_{\mu i} b^R_{\nu\kappa} = 0$$

für alle i, κ, μ, ν, also der erste Teil.

Zum Beweise des zweiten Teils muß k algebraisch abgeschlossen sein. Dann bilden wir wieder

$$D = \sum_R A'_R C \overline{A}_R, \text{ sodaß also } D\overline{A}_P = \overline{A}_P D \text{ ist,}$$

mit beliebigem C aus k. Nach Satz 9 folgt dann:

$$D = a_C E,$$

mit a_C aus k. Um a_C zu bestimmen, setzen wir wieder alle $c_{\mu\nu}$ bis auf eins gleich Null, das eine gleich 1. Dann wird III, 38

$$D = \left(\sum_R a^R_{\mu i} \overline{a}^R_{\nu\kappa} \right) = a_{\mu\nu} E$$

Diese Gleichung gibt zunächst

$$\sum_R a^R_{\mu i} \overline{a}^R_{\nu\kappa} = 0, \quad \text{wenn } i \neq \kappa;$$

ist aber $i = \kappa$, so wird für alle i

$$\sum_R a^R_{\mu i} \overline{a}^R_{\nu i} = a_{\mu\nu}.$$

Nun ist

$$a_{\mu\nu} = \sum_R a^R_{\mu i}\overline{a}^R_{\nu i} = \frac{1}{f}\sum_R \sum_{i=1}^{f} a^R_{\mu i}\overline{a}^R_{\nu i} = \frac{1}{f}\sum_R e_{\mu\nu} = \frac{g}{f}e_{\mu\nu},$$

weil ja $a_{\mu\nu}$ von i nicht abhängt und $\overline{A}_R$ zu A'_R reziprok ist. Damit ist auch der letzte Teil bewiesen.

Satz 12. *Ist Δ eine von der identischen Darstellung verschiedene irreduzible Darstellung in k, so ist die Summe der Matrizen von Δ gleich Null.*

Beweis: Wir wenden Satz 11 an auf den Fall $\Gamma = (1)$, die sogenannte *identische Darstellung* und ein davon verschiedenes irreduzibles Δ, sodaß also $\Delta \not\sim \overline{\Gamma} = \Gamma$ ist. Dann sagen die ersten Relationen von Satz 11 aus, daß die Summen aller Stellenzeilen von Δ gleich Null sind, w. z. b. w.

Satz 13. *Sind Γ, Δ irreduzible Darstellungen in k und $\Delta \not\sim \overline{\Gamma}$, so gilt*

$$\sum_R \chi_\Gamma(R)\chi_\Delta(R) = 0.$$

Ist ferner k algebraisch abgeschlossen, so gilt für ein in k irreduzibles Γ

$$\sum_R \chi_\Gamma(R)\chi_{\overline{\Gamma}}(R) = g.$$

Beweis: Setzt man in den ersten Relationen von Satz 11 speziell $i = \kappa, \mu = \nu$, so folgt nach Summation über i, μ:

$$\sum_R \sum_i a^R_{ii} \sum_\mu b^R_{\mu\nu} = \sum_R \chi_\Gamma(R)\chi_\Delta(R) = 0.$$

III, 39 Ebenso folgt für algebraisch abgeschlossenes k aus den zweiten Relationen von Satz 11 für $i = \kappa, \mu = \nu$:

$$\sum_R \sum_i a^R_{ii} \sum_\mu \overline{a}^R_{\mu\mu} = \sum_{i,\mu} \frac{g}{f} e_{i\mu} = g$$

$$\sum_R \chi_\Gamma(R)\chi_{\overline{\Gamma}}(R) = g,$$

w. z. b. w.

Satz 14. *Ist k algebraisch abgeschlossen, so sind zwei irreduzible Darstellungen in k dann und nur dann äquivalent, wenn ihre Charaktere übereinstimmen.*

Beweis: Stimmen die Charaktere überein:

$$\chi_\Gamma(R) = \chi_\Delta(R) \quad \text{für alle } R,$$

und wäre $\Gamma \not\sim \Delta$, so wäre

$$\sum_R \chi_{\overline{\Gamma}}(R)\chi_\Delta(R) = 0.$$

Es ist aber

$$\sum_R \chi_{\overline{\Gamma}}(R)\chi_\Delta(R) = \sum_R \chi_{\overline{\Gamma}}(R)\chi_\Gamma(R) = g.$$

Ist umgekehrt $\Gamma \sim \Delta$, so ist $\chi_\Gamma(R) = \chi_\Delta(R)$ für alle R nach Satz 3.

Satz 15. *Ist k algebraisch abgeschlossen, so läßt sich eine Darstellung auf eine und nur eine Weise in in k irreduzible Bestandteile zerlegen. Zwei beliebige Darstellungen sind dann und nur dann äquivalent, wenn ihre Charaktere übereinstimmen.*

Beweis: Sei

$$\Gamma \sim c_1\Gamma_1 + \cdots + c_r\Gamma_r \sim c_1'\Gamma_1 + \cdots + c_r'\Gamma_r$$

wo durch Aufnahme von Koeffizienten Null beiderseits dieselben irreduziblen Bestandteile erzeugt sind. Dann gilt

$$\chi_\Gamma(R) = \sum_i c_i\chi_{\Gamma_i}(R) = \sum_i c_i'\chi_{\Gamma_i}(R)$$

Multipliziert man beiderseits mit $\chi_{\overline{\Gamma}_\kappa}(R)$ und summiert über R, so folgt nach Satz 13 $c_\kappa = c_\kappa'$.

Hieraus folgt, daß das Übereinstimmen der Charaktere zweier Darstellungen das Übereinstimmen ihrer irreduziblen Bestandteile zur Folge hat, also ihre Äquivalenz in k. Das Umgekehrte folgt aus Satz 3.

Satz 16. *Ist k algebraisch abgeschlossen, so genügt der Grad f einer in k irreduziblen Darstellung der Relation* III, 40

$$f^2 \leqq g.$$

Es gibt nur endlich viele, nicht äquivalente irreduzible Darstellungen. Die Stellenzeilen einer irreduziblen Darstellung sind linear unabhängig in k. (siehe auch S. 44 Mitte!])

Beweis: Sei Γ eine irreduzible Darstellung in k vom Grade f. Bestünde zwischen ihren f^2 Stellenzeilen eine lineare Relation in k:

$$\sum_{i,\kappa} a_{i\kappa}^R c_{i\kappa} = 0 \quad \text{für alle } R,$$

so folgte durch Multiplikation mit dem Koeffizienten $\overline{a}_{\mu\nu}^R$ der Darstellung $\overline{\Gamma}$ und Summation über R nach Satz 11:

$$c_{\mu\nu} = 0.$$

Da es höchstens g linear unabhängige Stellenzeilen von g Größen in k geben kann, muß $f^2 \leqq g$ sein.

Ist nun A_P eine Matrix von Γ und $A_P^m = E$, so ist bekanntlich $\chi(A_P)$ die Summe der Wurzeln (Spur) der Gleichung

$$|A_P - xE| = 0$$

Die m–ten Potenzen dieser Wurzeln genügen

$$|E - yE| = 0,$$

also sind jene Wurzeln m–te Einheitswurzeln. $\chi(A_P)$ ist also eine Summe von f m–ten Einheitswurzeln. Wegen der Beschränktheit von f kommen also für $\chi(A_P)$ und damit für $\chi_\Gamma(P)$ nur endlich viele Werte in Betracht. Nach Satz 14 gibt es also nur endlich viele irreduzible Darstellungen von $\mathfrak{G}$ in k.

Satz 17. *Es seien $\mathfrak{C}_1, \dots, \mathfrak{C}_r$ die Klassen von $\mathfrak{G}$ und im Sinne der Komplexmultiplikation*

$$\mathfrak{C}_i \mathfrak{C}_\kappa = \sum_{\ell=1}^{r} c_{i\kappa\ell} \mathfrak{C}_\ell.$$

Ist dann Γ irreduzibel in k, wobei k algebraisch abgeschlossen, und f der Grad von Γ, h_i die Elementzahl von $\mathfrak{C}_i$ so gilt:

$$\frac{h_i}{f}\chi_\Gamma(\mathfrak{C}_i) \cdot \frac{h_\kappa}{f}\chi_\Gamma(\mathfrak{C}_\kappa) = \sum_{\ell=1}^{r} c_{i\kappa\ell} \frac{h_\ell}{f}\chi_\Gamma(\mathfrak{C}_\ell).$$

III, 41

Beweis: Natürlich ist $\chi_\Gamma(\mathfrak{C}_i)$ eindeutig definiert, da die Elemente einer Klasse $\mathfrak{C}_i$ entsprechenden Matrizen aus Γ durch Transformation auseinander hervorgehen, also gleiche Charaktere haben.

Sei nun C_i die Summe der Matrizen, die $\mathfrak{C}_i$ entsprechen. Dann gilt offenbar auch

$$C_i C_\kappa = \sum_{\ell=1}^{r} c_{i\kappa\ell} C_\ell.$$

Denn die entsprechende Komplexgleichung besagt, daß die $h_i \cdot h_\kappa$ Produkte $\mathfrak{C}_i \cdot \mathfrak{C}_\kappa$ dieselben sind, wie die $\sum_{\ell=1}^{r} c_{i\kappa\ell} h_\ell$ Summanden rechts. Also sind auch die Glieder rechts und links in der Matrizengleichung dieselben, also auch die Summen.

Ist dann A_P eine Matrix von Γ, so ist offenbar A_P mit C_i vertauschbar, denn es ist

$$A_P^{-1} C_i A_P = A_P^{-1} \sum_{R \text{ in } \mathfrak{C}_i} A_R A_P = \sum_{R \text{ in } \mathfrak{C}_i} A_{P^{-1}RP} = \sum_{R \text{ in } \mathfrak{C}_i} A_R = C_i,$$

weil $P^{-1}RP$ mit R die Klasse $\mathfrak{C}_i$ durchläuft. Nach 9 ist also

$$C_i = a_i E.$$

a_i bestimmt sich dann leicht:

$$\chi(C_i) = f a_i = \sum_{R \text{ in } \mathfrak{C}_i} \chi_\Gamma(R) = h_i \chi_\Gamma(\mathfrak{C}_i),$$

$$a_i = \frac{h_i}{f} \chi_\Gamma(\mathfrak{C}_i).$$

Aus obiger Relation für $C_i \cdot C_\kappa$ folgt dann durch Einsetzen von

$$C_i = \frac{h_i}{f} \chi_\Gamma(\mathfrak{C}_i) \cdot E$$

sofort die Behauptung.

Satz 18. *Sind $\Gamma = (a_{i\kappa}^R)$, $\Delta = (b_{i\kappa}^R)$ zwei Darstellungen der Grade n, m in k so ist auch*

$$\Gamma\Delta = \left(a_{i\mu}^R b_{\kappa\nu}^R\right); \quad \left.\begin{matrix}(i,\kappa)\\(\mu,\nu)\end{matrix}\right\} = (1,1), \ldots, (n,m)$$

eine Darstellung vom Grade $n \cdot m$ in k. Es ist dabei

$$\chi_{\Gamma\Delta}(R) = \chi_\Gamma(R) \chi_\Delta(R).$$

Beweis: Seien $(a_{i\mu}^R)$, $(b_{i\mu}^R)$, $(a_{i\mu}^S)$, $(b_{i\mu}^S)$ die R und S entsprechenden Matrizen in

III, 42 Γ und Δ. Dann ist das Produkt der R, S entsprechenden Matrizen in $\Gamma\Delta$:

$$(a_{i\mu}^R \; b_{\kappa\nu}^R) \; (a_{i\mu}^S \; b_{\kappa\nu}^S),$$

wo die Bogen die zu Zeilen und Spalten gekoppelten Indexpaare andeuten. Nach den Regeln des Matrizen Produktes ist dies gleich

$$\Big(\sum_{\varrho,\sigma} a_{i\varrho}^R \; b_{\kappa\sigma}^R \; a_{\varrho\mu}^S \; b_{\sigma\nu}^S\Big) = \Big(\sum_{\varrho} a_{i\varrho}^R \, a_{\varrho\mu}^S \;\cdot\; \sum_{\sigma} b_{\kappa\sigma}^R \, b_{\sigma\nu}^S\Big)$$

$$= \big(a_{i\mu}^{RS} \; b_{\kappa\nu}^{RS}\big).$$

Die Komposition in $\Gamma\Delta$ verläuft also isomorph zu $\mathfrak{G}$. Man hat nun noch zu zeigen, daß die Determinanten von $\Gamma\Delta$ nicht verschwinden. Es wäre leicht zu zeigen, daß sie die Produkte der von Γ und Δ sind. Jedoch genügt auch der Hinweis, daß offenbar dem Element E in $\Gamma\Delta$ die nm reihige Einheitsmatrix entspricht, und daher die Determinanten in $\Gamma\Delta$ nicht verschwinden, weil sie in hinreichend hoher Potenz gleich 1 sind.

Satz 19. *Ist $\Gamma_1, \ldots, \Gamma_{r'}$ ein vollständiges System irreduzibler Darstellungen in k und definiert man die Zahlen $g_{i\kappa\ell}$ durch die Relationen*

$$\Gamma_i \Gamma_\kappa \sim \sum_{\ell=1}^{r'} g_{i\kappa\ell} \Gamma_\ell,$$

so gilt

$$\chi_{\Gamma_i}(R) \chi_{\Gamma_\kappa}(R) = \sum_{\ell=1}^{\ell'} g_{i\kappa\ell} \chi_{\Gamma_\ell}(R)$$

Beweis: Folgt unmittelbar aus Satz 4 und 18. Die Frage, ob es nur endlich viele Γ_i in *beliebigen* k gibt, und ob die Zerlegung in irreduzible Bestandteile *eindeutig* ist, hat hiermit nichts zu tun. Jedenfalls läßt sich jedes Produkt $\Gamma_i \Gamma_\kappa$ in irreduzible Bestandteile in k aufspalten, und dann gilt eben die genannte Relation.

Für die irreduziblen Darstellungen 1. Grades der Abelschen Gruppen in Körpern geeigneter Einheitswurzeln geben die Multiplikationstheoreme von Satz 17 und 19 die bekannten Multiplikationstheoreme der Charaktere Abelscher Gruppen. Das Produkt zweier Klassen (Elemente) ist hier ein bestimmtes drittes

III, 43 Element, und das Produkt zweier Darstellungen eine bestimmte dritte.

Ist $\Gamma = (A_R)$ eine Darstellung von $\mathfrak{G}$ und x_R den Gruppenelementen entsprechende Variable, so bezeichnen wir mit Γ auch die Matrix aus Linearformen

$$\Gamma = \left(\sum_R A_R x_R \right),$$

die die *Gruppenmatrix* von Γ heißt.

Satz 20. *Die durch hintere Multiplikation der Elemente von $\mathfrak{G}$ mit einem bestimmten Element gelieferte Permutationsdarstellung von $\mathfrak{G}$, die in Matrizen geschrieben offenbar eine Darstellung im Körper der rationalen Zahlen ist, und die die reguläre Darstellung von $\mathfrak{G}$ heißt, hat die Gruppenmatrix*

$$\Gamma = (x_{P^{-1}Q}),$$

wo P die Zeilen, Q die Spalten von Γ auf die Gruppenelemente bezieht, die in einer festen Reihenfolge vorliegend anzusehen sind.

Beweis: Dem Gruppenelement R entspricht eine Matrix, die in der durch P bestimmten Zeile an derjenigen Stelle eine 1 besitzt, für die $P^{-1}Q = R$, d. h. $Q = PR$ ist, während immer alle anderen Elemente der betr. Zeile Null sind. Das ist also eine Permutationsmatrix, und sie entspricht gerade derjenigen Permutation der in einer festen Reihenfolge vorliegenden Gruppenelemente, die durch hintere Multiplikation mit R erzeugt wird.

Satz 21. *Ist k algebraisch abgeschlossen, so enthält die reguläre Darstellung von $\mathfrak{G}$ jede irreduzible Darstellung in $\mathfrak{G}$ und zwar so oft, als deren Grad angibt. Für die Grade f_i der r' irreduziblen Darstellungen in k gilt somit*

$$\sum_{i=1}^{r'} f_i^2 = g$$

Beweis: Sei Γ die reguläre Darstellung. Da k sicher den Körper der rationalen Zahlen enthält, ist Γ Darstellung in k. Es sei nun

$$\Gamma \sim n_1\Gamma_1 + \cdots + n_{r'}\Gamma_{r'}$$

die nach Satz 15 eindeutige Zerlegung von Γ in k, wobei die sämtlichen irreduziblen Bestandteile in k, nötigenfalls mit dem Koeffizienten Null aufgeschrieben

III, 44

sind (Nach Satz 16 sind es nur endlich viele). Es ist dann

$$\chi_\Gamma(R) = \sum_{i=1}^{r'} n_i \chi_{\Gamma_i}(R)$$

Nun ist ersichtlich

$$\chi_\Gamma(E) = g$$
$$\chi_\Gamma(R) = 0, \quad \text{wenn } R \neq E$$

Multiplizieren wir also obige Gleichung mit $\chi_{\overline{\Gamma}_\kappa}(R)$ und summieren über R, so folgt nach Satz 13

$$g\chi_{\overline{\Gamma}_\kappa}(E) = gf_\kappa = n_\kappa g, \quad \text{also}$$
$$n_\kappa = f_\kappa.$$

Die Tatsache, daß es nur endlich viele irreduzible Darstellungen geben kann, folgt übrigens mit aus diesem Schluß, sodaß Satz 16 mit Beweis erspart werden kann. Denn wäre ein Γ_κ nicht in Γ enthalten, so folgte hier der Widerspruch $gf_\kappa = 0$.

Satz 22. *Es sei K der Körper aller algebraischen Zahlen, k irgendein algebraisch abgeschlossener Körper der Charakteristik 0, also Oberkörper von K. Dann ist ein vollständiges System irreduzibler Darstellungen in K auch ein solches in k, sodaß es für die Darstellungstheorie genügt, K zugrundezulegen.*

Der Beweis ist so nicht richtig und erfordert nähere Ausführung mit den Charakter-Relationen für K und k.

Beweis: Die sämtlichen irreduziblen Darstellungen in k, K folgen durch Zerlegung der regulären Darstellung in k, K in irreduzible Bestandteile. Ist diese Zerlegung für K bereits ausgeführt, so ist also auch für k (als Oberkörper von K) eine teilweise Zerlegung gewonnen. Wäre diese noch nicht die vollständige, so müßte jedenfalls nach dem Eindeutigkeitssatz die vollständige Zerlegung in k durch weitere Aufspaltung der irreduziblen Bestandteile von K in solche von k entstehen. Hierbei würden sich die Grade der Bestandteile in K gegenüber denen in k erniedrigen. Damit ihre Quadratsumme g bleibt müßte sich also ihre Anzahl vergrößern, d. h. es könnte nicht jeder irreduzible Bestandteil in K nur ein gewisses Vielfaches *eines* irreduziblen Bestandteiles in k sein.

Im nächsten Satz wird sich aber ergeben, daß die Anzahl r' der irreduziblen Bestandteile der regulären Darstellung, also die Anzahl der verschiedenen irreduziblen Darstellungen überhaupt für jeden algebraisch abgeschlossenen Körper gleich der Anzahl r der Klassen von $\mathfrak{G}$ ist. Daher kann in k keine Zerfällung mehr eintreten. III, 45

Satz 23. *Ist k algebraisch abgeschlossen, $\Gamma_1, \ldots, \Gamma_{r'}$ ein vollständiges System irreduzibler Darstellungen der Grade $f_1, \ldots, f_{r'}$ in k, $\mathfrak{C}_1, \ldots, \mathfrak{C}_r$ die Klassen in $\mathfrak{G}$ mit den Elementzahlen $h_1, \ldots, h_r$, so gelten die Relationen*

$$\sum_{i=1}^{r} h_i \chi_{\Gamma_\nu}(\mathfrak{C}_i) \chi_{\Gamma_\mu}(\mathfrak{C}_i) = \begin{cases} 0 & \textit{wenn} \quad \Gamma_\mu \not\sim \overline{\Gamma}_\nu \\ g & \quad '' \quad\; \Gamma_\mu \sim \overline{\Gamma}_\nu \end{cases}$$

$$\sum_{i=1}^{r'} h_i \chi_{\Gamma_\nu}(\mathfrak{C}_i) \chi_{\Gamma_\nu}(\mathfrak{C}_\kappa) = \begin{cases} 0 & \textit{wenn} \quad \mathfrak{C}_i \neq \overline{\mathfrak{C}}_\kappa \\ g & \quad '' \quad\; \mathfrak{C}_i = \overline{\mathfrak{C}}_\kappa \end{cases}$$

Dabei bezeichnet $\overline{\mathfrak{C}}_\kappa$ die zu $\mathfrak{C}_\kappa$ reziproke Klasse. Die Matrix

$$\Big(h_\kappa \chi_{\Gamma_i}(\mathfrak{C}_\kappa)\Big); \qquad \begin{pmatrix} i = 1, 2, \ldots\, r' \\ \kappa = 1, 2, \ldots\, r \end{pmatrix}$$

hat den Typus $r \cdot r$, d. h. $r = r'$ und von Null verschiedene Determinante.

Beweis: Ist $\overline{\mathfrak{C}}_i$ die aus den reziproken Elementen von $\mathfrak{C}_i$ gebildete Klasse, so ist

$$\mathfrak{C}_i \overline{\mathfrak{C}}_i = h_i \mathfrak{C}_1 + \cdots, \quad \text{d. h.} \quad c_{i\bar{i}1} = h_i$$

Ist dagegen $\mathfrak{C}_\kappa \neq \overline{\mathfrak{C}}_i$, so ist

$$\mathfrak{C}_i \mathfrak{C}_\kappa = 0 \cdot \mathfrak{C}_1 + \cdots, \quad \text{d. h.} \quad c_{i\kappa 1} = 0.$$

Nun ist nach Satz 17

$$h_i \chi_{\Gamma_\nu}(\mathfrak{C}_i)\, h_\kappa \chi_{\Gamma_\nu}(\mathfrak{C}_\kappa) = f_\nu \sum_{\ell=1}^{r} c_{i\kappa\ell} h_\ell \chi_{\Gamma_\nu}(\mathfrak{C}_\ell)$$

Durch Summation über ν folgt:

$$\sum_{\nu=1}^{r'} h_i h_\kappa \chi_{\Gamma_\nu}(\mathfrak{C}_i)\chi_{\Gamma_\nu}(\mathfrak{C}_\kappa) = \sum_{\ell=1}^{r} c_{i\kappa\ell} h_\ell \sum_{\nu=1}^{r'} f_\nu \chi_{\Gamma_\nu}(\mathfrak{C}_\ell)$$
$$= \sum_{\ell=1}^{r} c_{i\kappa\ell} h_\ell \chi_\Gamma(\mathfrak{C}_\ell),$$

III, 46 nach Satz 21, wenn Γ die reguläre Darstellung bezeichnet. Da $\chi_\Gamma(\mathfrak{C}_\ell)$ nur für $\mathfrak{C}_1$ von Null verschieden und gleich g ist, folgt

$$\sum_{\nu=1}^{r'} h_i h_\kappa \chi_{\Gamma_\nu}(\mathfrak{C}_i)\chi_{\Gamma_\nu}(\mathfrak{C}_\kappa) = g c_{i\kappa 1} = \begin{cases} 0 & \text{wenn} \quad \mathfrak{C}_\kappa \neq \overline{\mathfrak{C}}_i \\ g h_\kappa & \quad = \quad \mathfrak{C}_\kappa = \overline{\mathfrak{C}}_i\,. \end{cases}$$

Damit sind die zweiten Relationen bewiesen. Die ersten sind einfach die von Satz 13.

Aus den beiden Relationensystemen folgt nun ohne weiteres, daß die Zeilen und Spalten der rechteckigen Matrix

$$\big(h_\kappa \chi_{\Gamma_i}(\mathfrak{C}_\kappa)\big); \quad \begin{pmatrix} i = 1, 2, \dots, r' \\ \kappa = 1, 2, \dots, r \end{pmatrix}$$

linear unabhängig sind. Denn bestünde eine Relation

$$\sum_{\nu=1}^{r'} p_\nu h_i \chi_{\Gamma_\nu}(\mathfrak{C}_i) = 0 \quad \text{für alle } i,$$

so folgte durch Multiplikation mit $\chi_{\overline{\Gamma}_\mu}(\mathfrak{C}_i)$ und Summation über i: $g p_\mu = 0$, d. h. $p_\mu = 0$. Bestünde eine Relation

$$\sum_{i=1}^{r} p_i h_i \chi_{\Gamma_\nu}(\mathfrak{C}_i) = 0 \quad \text{für alle } \nu,$$

so folgte durch Multiplikation mit $\chi_{\Gamma_\nu}(\overline{\mathfrak{C}}_\kappa)$ und Summation über ν: $g p_\kappa = 0$, d. h. $p_\kappa = 0$.

Also ist $r = r'$ und $|h_\kappa \chi_{\Gamma_i}(\mathfrak{C}_\kappa)| \neq 0$, w. z. b. w.

Es bezeichne fortan K *den Körper aller algebraischen Zahlen*, auf den und auf dessen Unterkörper wir uns nach Satz 22 nunmehr beschränken können.

Satz 24. *Die Grade f_i der r irreduziblen Bestandteile in K sind Teiler von g.*

Beweis: Nach Satz 17 gilt, wenn zur Abkürzung

$$x_i = \frac{h_i}{f}\chi_\Gamma(\mathfrak{C}_i)$$

gesetzt wird, wobei Γ eine in K irreduzible Darstellung f–ten Grades bezeichnet:

$$x_i x_\kappa = \sum_{\ell=1}^{r} c_{i\kappa\ell} x_\ell$$

mit ganzzahligen Koeffizienten $c_{i\kappa\ell}$. Das bedeutet, daß für jedes feste κ das betr. x_κ Wurzel der algebraischen Gleichung

$$|C_\kappa - x_\kappa E| = 0$$

ist, wenn C_κ die Matrix III, 47

$$C_\kappa = (c_{i\kappa\ell}); \quad \begin{pmatrix} i = 1, 2, \ldots, r \\ \ell = 1, 2, \ldots, r \end{pmatrix}$$

bedeutet. Diese Gleichung für x_κ ist ganzzahlig und der höchste Koeffizient ± 1. Daher ist x_κ eine *ganze* algebraische Zahl aus K.

Nun ist

$$\sum_{\kappa=1}^{r} x_\kappa \chi_{\overline{\Gamma}}(\mathfrak{C}_\kappa) = \frac{1}{f}\sum_{\kappa=1}^{r} h_\kappa \chi_\Gamma(\mathfrak{C}_\kappa)\chi_{\overline{\Gamma}}(\mathfrak{C}_\kappa) = \frac{g}{f}$$

Da nun die Charaktere $\chi_{\overline{\Gamma}}(\mathfrak{C}_\kappa)$ als Summen von Einheitswurzeln ganze algebraische Zahlen sind, ist $\frac{g}{f}$ algebraisch ganz, dh. ganz rational, w. z. b. w.

Überdies hat sich ergeben:

Satz 25. *Ist Γ eine irreduzible Darstellung in K, $\mathfrak{C}$ eine Klasse von $\mathfrak{G}$ mit h Elementen und f der Grad von Γ, so ist $\frac{h}{f}\chi_\Gamma(\mathfrak{C})$ eine ganze algebraische Zahl.*

Wir führen nun hyperkomplexe Zahlen ein, indem wir Ausdrücke

$$\xi = \sum_R a_R R$$

bilden, wo die a_R irgendwelche Zahlen aus K sind. Definiert man für

$$\begin{aligned} \xi &= \sum_R a_R R \\ \eta &= \sum_R b_R R \end{aligned}$$

Summe, Differenz und Produkt durch

$$\begin{aligned} \xi \pm \eta &= \sum_R (a_R \pm b_R) R \\ \xi \cdot \eta &= \sum_{R,S} a_R b_S RS \end{aligned}$$

so gelten die gewöhnlichen Rechenregeln der Addition und Multiplikation bis auf das kommutative Gesetz der letzteren. Zwei hyperkomplexe Zahlen heißen dann und nur dann gleich, wenn ihre Koeffizienten übereinstimmen.

III, 48

Ist $\Gamma = (A_R) = \left(a_{i\kappa}^R\right)$ eine Darstellung in K, so definiert sie ein System hyperkomplexer Zahlen

$$\xi_{i\kappa} = \sum_R a_{i\kappa}^R R,$$

deren Koeffizienten die Stellenzeilen von Γ sind. Die Matrix Ξ der $\xi_{i\kappa}$ ist

$$\Xi = (\xi_{i\kappa}) = \left(\sum_R a_{i\kappa}^R R\right) = \sum_R A_R R.$$

Satz 26. *Ist Γ eine Darstellung in k, Ξ die zugeordnete Matrix hyperkomplexer Zahlen, so gilt für eine beliebige Matrix A_R aus Γ:*

$$\begin{aligned} \Xi A_R^{-1} &= \Xi R \\ A_R^{-1} \Xi &= R \Xi. \end{aligned}$$

Beweis: Es ist

$$\begin{aligned} \Xi &= \sum_S A_S S \\ \Xi A_R^{-1} &= \sum_S A_{SR^{-1}} S = \sum_S A_S SR = \Xi R \\ A_R^{-1} \Xi &= \sum_S A_{R^{-1}S} S = \sum_S A_S RS = R\Xi. \end{aligned}$$

Dieser Satz läßt sich auch so aussprechen:

Satz 27. *Bei rechtsseitiger Multiplikation mit R erfahren die Zeilen von Ξ die Substitution $\overline{A}_R$.*
Bei linksseitiger Multiplikation mit R^{-1} erfahren die Spalten von Ξ die Substitution A_R.

Ist nämlich Z_i die i–te Zeile, H_κ die κ–te Spalte von Ξ so folgt aus Satz 26

$$\begin{aligned} Z_i A_R^{-1} &= Z_i R \\ A_R \mathsf{H}_\kappa &= R^{-1}\mathsf{H}_\kappa . \end{aligned}$$

Die zweite Relation gibt unmittelbar die Aussage des Satzes, da $A_R\mathsf{H}_\kappa$ die der Substitution A_R unterworfenen Elemente H_κ bedeutet. Die erste Relation ergibt

$$\overline{A}_R Z_i' = Z_i' R$$

wenn Z_i' die Zeile Z_i als Spalte bedeutet, und hat somit die Bedeutung der ersten Aussage des Satzes. III, 49

Satz 28. *Zwischen den hyperkomplexen Zahlen, die einer in K irreduziblen Darstellung Γ entsprechen, bestehen die Beziehungen:*

$$\begin{aligned} \xi_{i\kappa}\cdot\xi_{\mu\nu} &= 0 \quad \text{für } \kappa \neq \mu \\ \xi_{i\kappa}\cdot\xi_{\kappa\nu} &= \frac{g}{f}\xi_{i\nu} \end{aligned}$$

wenn f der Grad von Γ ist.

Sind Γ, Δ zwei in irgendeinem Unterkörper von K irreduzible Darstellungen und $\Gamma \not\sim \Delta$, so bestehen zwischen den hyperkomplexen Zahlen $\xi_{i\kappa}$ von Γ und $\eta_{i\kappa}$ von Δ die Relationen

$$\xi_{i\kappa}\eta_{\mu\nu} = 0$$

Beweis: 1.) Ist Γ irreduzibel in K und $\Xi = (\xi_{i\kappa})$ die zugeordnete hyperkomplexe Matrix, so ist

$$\Xi R = \Xi A_R^{-1}, \quad \text{also} \quad \Xi\left(\sum_R a_{\mu\nu}^R R\right) = \Xi\left(\sum_R a_{\mu\nu}^R A_R^{-1}\right)$$

d. h.

$$\Xi\xi_{\mu\nu} = \Xi\left(\sum_R a^R_{\mu\nu}\left(\overline{a}^R_{i\kappa}\right)'\right).$$

Nun ist nach Satz 11 die Matrix (i Zeilen, κ Spalten)

$$\sum_R a^R_{\mu\nu}(\overline{a}^R_{i\kappa})' = \left(\sum_R a^R_{\mu\nu}\overline{a}^R_{i\kappa}\right)' = \frac{g}{f}E_{\nu\mu}$$

III, 50

wo $E_{\nu\mu}$ die Matrix bezeichnet, die nur in der ν–ten Zeile und μ–ten Spalte eine 1, sonst überall Nullen hat. Es ist dann

$$\Xi\xi_{\mu\nu} = \frac{g}{f}\Xi E_{\nu\mu} = \frac{g}{f}\cdot\left(\begin{array}{c}\nu \text{ te Spalte von } \Xi\\ \text{an Stelle der } \mu\text{–ten Spalte}\end{array}\right).$$

Daraus folgen sofort durch Koeffizientenvergleich die Relationen des Satzes.
2.) Sind Γ, Δ irreduzibel in irgendeinem Körper k, (wobei es genügt k auf Unterkörper von K oder K selbst zu beschränken), so folgt genau ebenso aus Satz 11 und 26:

$$\begin{aligned}\Xi R &= \Xi A_R^{-1}\\ \Xi\left(\sum_R b^R_{\mu\nu}R\right) &= \Xi\eta_{\mu\nu} = \Xi\sum_R b^R_{\mu\nu}\left(\overline{a}^R_{i\kappa}\right)'\\ &= \Xi\left(\sum_R b^R_{\mu\nu}\overline{a}^R_{i\kappa}\right)' = \Xi\cdot 0 = 0,\end{aligned}$$

wenn $\Gamma \not\sim \Delta$.

Satz 29. *Ist $\Gamma_1, \ldots, \Gamma_r$ das vollständige System der irreduzibeln Darstellungen in K; $\Xi_1, \ldots, \Xi_r$ die zugeordneten hyperkomplexen Matrizen, so sind die g Stellenzeilen der Γ_p, oder was dasselbe bedeutet, die g hyperkomplexen Zahlen $\xi^{(p)}_{i\kappa}$ der Ξ_p linear unabhängig in K.*

Beweis: Bestünde eine Relation

$$\sum_{i,\kappa,p} c^{(p)}_{i\kappa}\xi^{(p)}_{i\kappa} = 0,$$

so folgte durch Multiplikation mit $\xi_{\mu\nu}^{(q)}$ nach Satz 28

$$\frac{g}{f_q}\sum_i c_{i\mu}^{(q)}\xi_{i\nu}^{(q)} = 0,$$

d. h. eine Relation zwischen f_q Stellenzeilen von Γ_q. Diese sind aber linear unabhängig, wie schon aus den Relationen von Satz 11 folgt, und in Satz 16 bewiesen wurde.

Satz 30. *Ist* Γ *die reguläre Gruppenmatrix,* N *die aus den* g *Stellenzeilen der sämtlichen irreduziblen Bestandteile in* K *gebildete Matrix, so ist* $N\Gamma N^{-1}$ *die vollständig reduzierte Gruppenmatrix.* III, 51

Beweis: Die reguläre Darstellung Γ entsteht als die Substitutionsgruppe, die die Gruppenelemente $E, R, \ldots$ bei hinterer Multiplikation mit einem festen erfahren. Ersetzt man die Gruppenelemente durch die g aus den Stellenzeilen der irreduziblen Darstellungen gebildeten Linearformen (hyperkomplexen Zahlen), so erfahren diese Linearformen die mit N transformierten Substitutionen bei hinterer Multiplikation mit den Gruppenelementen: In Formeln:

Sind $R_1, \ldots, R_g$ die g Gruppenelemente, und

$$R_i S = A_S(R_\kappa)$$

die durch hintere Multiplikation mit S erzeugte Permutationssubstitution A_S von Γ, so ist

$$\xi_i S = N(R_i)\cdot S = N(R_i S) = NA_S(R_\kappa) = NA_S N^{-1}\big(N(R_\kappa)\big), \quad \text{also}$$
$$\xi_i S = NA_S N^{-1}(\xi_\kappa)$$

die Substitution, die die g hyperkomplexen Zahlen ξ_i erfahren, wenn N die Matrix ihrer Koeffizienten, d. h. die Matrix der g Stellenzeilen der irreduziblen Darstellungen in K ist.

Denkt man sich nun die g Stellenzeilen nach den irreduziblen Darstellungen und innerhalb dieser nach deren Zeilen geordnet, so folgen hintereinander 1. – f_1 te Zeile von Γ_1, 1. – f_2 te Zeile von Γ_2,... d. h. 1. – f_1–te Zeile von Ξ_1, 1. – f_2 te Zeile von Ξ_2,... Die f_ν Zeilen jedes Ξ_ν erfahren nun bei hinterer Multiplikation mit S gerade die Substitution $\overline{A}_S^{(\nu)}$ aus $\overline{\Gamma}_\nu$. Daher ist NA_SN^{-1} zerlegt in genau die irreduzibeln Bestandteile $\overline{\Gamma}_1, \ldots, \overline{\Gamma}_r$, jeder so oft als sein Grad angibt, gesetzt, also ist Γ vollständig reduziert, w. z. b. w.

III, 52

Satz 31. *Sind* $\Gamma = \left(a_{i\kappa}^R\right)$, $\Delta = \left(b_{i\kappa}^R\right)$ *zwei äquivalente irreduzible Darstellungen vom Grade* f *in* K *und*

$$U^{-1}\Gamma U = \Delta,$$

so berechnen sich die Koeffizienten $u_{i\kappa}$ *von* U *aus*

$$\frac{g}{f} u_{i\kappa} u_{\mu\nu} = \sum_R a_{i\nu}^{R^{-1}} b_{\mu\kappa}^R$$

eindeutig bis auf einen gemeinsamen Faktor, wenn $U^{-1} = (u_{i\kappa})$ *ist.*

Beweis: Sind $\Xi = (\xi_{i\kappa})$ und $\mathsf{H} = (\eta_{i\kappa})$ die zugehörigen Matrizen hyperkomplexer Größen, so muß sein

$$U^{-1}\Xi U = \mathsf{H},$$

d. h.

$$\sum_{\mu,\nu} u_{i\mu}^{\kappa} \xi_{\mu\nu} u_{\nu\kappa} = \eta_{i\kappa}$$

Es wird dann also nach Satz 28:

$$\eta_{i\kappa}\xi_{\ell m} = \frac{g}{f} \sum_\mu u_{i\mu}\xi_{\mu m} u_{\ell\kappa}.$$

Wir bilden rechts und links den Koeffizienten von E:

$$\sum_R b_{i\kappa}^R a_{\ell m}^{R^{-1}} = \frac{g}{f} u_{im} u_{\ell\kappa},$$

da $\xi_{\mu m} = \sum a_{\mu m}^R R$ nur für $\mu = m$ einen von Null verschiedenen Koeffizienten $a_{mm}^E = 1$ hat (A_E ist die Einheitsmatrix). Durch Umschreibung der Indizes folgt sofort die Behauptung. Natürlich ist nach Satz 9 U bis auf einen Faktor bestimmt. Um U zu berechnen, suche man eine Summe $\sum_R a_{i\nu}^{R^{-1}} b_{\mu\kappa}^R \neq 0$, setze dann $u_{\mu\nu} = 1$ und berechne bei festgehaltenem μ, ν durch Variation von i, κ alle anderen $u_{i\kappa}$.

Satz 32. *Es sei H eine Untergruppe von $\mathfrak{G}$ vom Index n und*

$$\mathfrak{G} = \sum_{i=1}^{n} \mathfrak{H} T_i$$

Sei dann

$$\Delta = (A_R)\,; \quad R \text{ in } \mathfrak{H}$$

eine Darstellung von $\mathfrak{H}$ in k vom Grade f. Ist dann für ein Element S aus $\mathfrak{G}$ allgemein

$$T_i S = R_i^{(S)} T_{p_i}\,; \quad R_i^{(S)} \text{ in } \mathfrak{H}\,; \quad (i = 1, 2, \ldots n)$$

und ordnet man S diejenige Matrix vom Grade $n \cdot f$ zu, die, in n Teilzeilen und Spalten der Ausdehnung f zerlegt, in der i–ten Zeile und p_i–ten Spalte die Matrix $A_{R_i^{(S)}}$ hat, und sonst lauter Nullen, so entsteht eine „imprimitive“, „transitive“ Darstellung Γ_Δ von $\mathfrak{G}$ in k vom Grade $n \cdot f$, deren Teilmatrizen nach Konstruktion aus Δ stammen. Ist Δ die reguläre Darstellung, so auch Γ_Δ. Ist Δ die identische Darstellung, so ist Γ_Δ eine Permutationsgruppe.
Die Gruppenmatrix von Γ_Δ Ist in symbolischer Bezeichnung

$$\Gamma_\Delta = \left(T_i^{-1} \Delta T_\kappa\right)\,; \quad (i, \kappa = 1, \ldots, n),$$

wo

$$T_i^{-1} \Delta T_\kappa = T_i^{-1} \left(\sum_{R \text{ in } \mathfrak{H}} A_R x_R \right) T_\kappa = \sum_{R \text{ in } \mathfrak{H}} A_R x_{T_i^{-1} R T_\kappa}$$

gesetzt ist.[1]

III, 53

Beweis: Wir weisen den Isomorphismus von Γ_Δ mit $\mathfrak{G}$ nach. Ist

$$T_i S = R_i^{(S)} T_{p_i}\,; \quad T_i T = R_i^{(T)} T_{q_i}\,; \quad (i = 1, 2, \ldots n)$$

so liefert das Produkt der beiden Matrizen von Γ_Δ, die S und T entsprechen in der i–ten Zeile nur an der Stelle etwas von Null verschiedenes, wo in der T entsprechenden Matrix eine Spalte etwas an p_i–ter Stelle enthält, also beim

[1]Randbemerkung von Hasse: *Artin Hambg. Abh. 3, L-Reihen–Arbeit*

inneren Produkt mit der q_{p_i}–ten Spalte von T. Und an dieser Stelle steht

$$R_i^{(S)} \cdot R_{p_i}^{(T)} \quad \text{in Zeile } i, \text{ Spalte } q_{p_i}$$

Andererseits steht an dieser Stelle in der ST entsprechenden Matrix dasselbe, und sonst in der i–ten Zeile nichts. Denn es ist

$$T_i ST = R_i^{(S)} T_{p_i} T = R_i^{(S)} R_{p_i}^{(T)} T_{q_{p_i}} .$$

Damit ist gezeigt, daß Γ_Δ eine Darstellung von $\mathfrak{G}$ in k vom Grade $n \cdot f$ ist, deren f–reihige Teilmatrizen aus Δ stammen. Daß der identischen Darstellung so eine Permutationsgruppe Γ_Δ, und zwar die durch die Permutationen

$$\begin{pmatrix} \mathfrak{H} T_i \\ \mathfrak{H} T_i S \end{pmatrix}$$

erzeugte, entspricht, ist klar. Um auch die Behauptung bezüglich der regulären Darstellung zu beweisen, weisen wir zuerst nach, daß

$$\Gamma_\Delta = \left(T_i^{-1} \Delta T_\kappa \right)$$

in erklärtem Sinne ist. In der Tat ist der Koeffizient von x_S hierin eine Matrix, die in der i–ten Zeile nur für das κ eine Matrix stehen hat, für das $T_i^{-1} R T_\kappa = S$, d. h. $T_i S = R T_\kappa$ ist, und zwar dann die Matrix A_R, wie es sein muß. Ist nun speziell

$$\Delta = (x_{P^{-1}Q}) ; \quad P, Q \text{ in } \mathfrak{H}$$

III, 54 so wird einfach

$$\Gamma_\Delta = \left(x_{T_i^{-1} P^{-1} Q T_\kappa} \right) ; \quad \begin{pmatrix} P, Q \text{ in } \mathfrak{H} \\ i, \kappa = 1, \dots n \end{pmatrix} .$$

Da aber QT_κ und PT_i so gerade die ganze Gruppe $\mathfrak{G}$ durchlaufen, entsteht gerade die reguläre Darstellung von $\mathfrak{G}$, w. z. b. w.

Satz 33. *Es sei Γ eine solche Darstellung von $\mathfrak{G}$ in k, die in n transitiv verbundene, Systeme der Imprimitivität vom Grade f zerfällt, und $\mathfrak{H}$ diejenige Untergruppe von $\mathfrak{G}$, bei der etwa das System der ersten Zeile auch in der ersten Spalte steht. Dann ist Γ der aus derjenigen Darstellung Δ von $\mathfrak{H}$ entspringenden Darstellung Γ_Δ äquivalent, die durch die genannten Teilmatrizen von Γ geliefert wird.*

Beweis: Sei

$$\mathfrak{G} = \sum_{i=1}^{n} \mathfrak{H} T_i\,, \quad (T_1 = E)$$

sodaß der Nebengruppe $\mathfrak{H}T_i$ in Γ Matrizen entsprechen, die in erster Zeile nur an der i–ten Stelle besetzt sind, und seien speziell C_i die dort stehenden Matrizen für die T_i. Dann transponieren wir Γ mit der Matrix aus k:

$$\begin{pmatrix} E & & & \\ & C_2^{-1} & & \\ & & \ddots & \\ & & & C_n^{-1} \end{pmatrix},$$

sodaß nunmehr die T_i entsprechenden Matrizen in der ersten Zeile an i–ter Stelle E haben.

Sei nunmehr $\Delta = (A_R)$ die durch die linken oberen Teilmatrizen gelieferte Darstellungen von $\mathfrak{H}$ in k, (die übrigens bei der Transformation ganz unberührt blieb), und S ein Element von $\mathfrak{G}$ mit

$$T_i S = R_i^{(S)} T_{p_i}.$$

S habe an $i - \kappa$–ter Stelle die Matrix B. Dann hat $T_i S$ an $1 - \kappa$–ter Stelle B, und da es gleich $R_i^{(S)} T_{p_i}$ ist, muß $p_i = \kappa$ und $B = A_{R_i^{(S)}}$ sein. Damit ist die Behauptung bewiesen.

Satz 34. *Ist $\Gamma_1, \dots, \Gamma_r$ das System der irreduziblen Darstellungen von $\mathfrak{G}$ in K, $\Delta_1, \dots \Delta_s$ dasselbe für $\mathfrak{H}$ und bezeichnet allgemein Γ_{Δ_ν} die nach Satz 32 erzeugte imprimitive, transitive Darstellung, Δ_{Γ_μ} die auf $\mathfrak{H}$ bezüglichen Matrizen von Γ_μ, so gilt gleichzeitig*

$$\begin{aligned} \Gamma_{\Delta_\nu} &= k_{\mu\nu}\Gamma_\mu + \cdots \\ \Delta_{\Gamma_\mu} &= k_{\mu\nu}\Delta_\nu + \cdots \end{aligned}$$

d. h. zusammenfassend:

$$\Gamma_{\Delta_\nu} = \sum_{\mu=1}^{r} k_{\mu\nu}\Gamma_\mu$$

$$\Delta_{\Gamma_\mu} = \sum_{\nu=1}^{s} k_{\mu\nu}\Delta_\nu .$$

III, 55 *Beweis*: Für S aus $\mathfrak{G}$ ist:

$$\sum_{S \text{ in } \mathfrak{G}} \chi_{\Gamma_{\Delta_\nu}}(S)\chi_{\overline{\Gamma}_\mu}(S) = k_{\mu\nu} g,$$

wenn $\Gamma_{\Delta_\nu} = k_{\mu\nu}\Gamma_\mu + \cdots$ gesetzt wird. Die Summe links läßt sich aber noch auf eine zweite Art berechnen. Es ist ja

$$\Gamma_{\Delta_\nu} = \left(T_i^{-1}\Delta_\nu T_\kappa\right) = \left(\sum_{R \text{ in } \mathfrak{H}} A_R x_{T_i^{-1}RT_\kappa}\right)$$

wenn $\mathfrak{G} = \sum_{i=1}^n \mathfrak{H}T_i$ die Zerlegung von $\mathfrak{G}$ nach der Δ_ν zugeordneten Gruppe $\mathfrak{H}$ ist, und $\Delta_\nu = (A_R)$ gesetzt wird. Damit hier eine Matrix in der Diagonale steht, muß

$$T_i^{-1}RT_i = S$$

sein, wenn die dem Element S von $\mathfrak{G}$ entsprechende Matrix von Γ_{Δ_ν} betrachtet wird. Die i–te Zeile liefert also alle und nur die A_R als Beitrag zu den Diagonalen der Elemente S von $\mathfrak{G}$, für die S in $T_i^{-1}\mathfrak{H}T_i$ liegt. Wir zerlegen nun

$$\sum_{S \text{ in } \mathfrak{G}} \chi_{\Gamma_{\Delta_\nu}}(S)\chi_{\overline{\Gamma}_\mu}(S) = \sum_{i=1}^n \sum_S [\text{Beitrag der } i\text{–ten Zeile zu } \chi_{\Gamma_{\Delta_\nu}}(S)]\chi_{\overline{\Gamma}_\mu}(S).$$

Für den Beitrag der i–ten Zeile kommen nur die S in $T_i^{-1}\mathfrak{H}T_i$ in Frage, und jedes solche $S = T_i^{-1}RT_i$ mit dem Beitrag A_R, also mit dem Charakter $\chi_{\Delta_\nu}(R)$. Also wird

$$\begin{aligned}
\sum_{S \text{ in } \mathfrak{G}} \chi_{\Delta_\nu}(S)\chi_{\overline{\Gamma}_\mu}(S) &= \sum_{i=1}^n \sum_{S \text{ in } T_i^{-1}\mathfrak{H}T_i} \chi_{\Delta_\nu}\left(T_iST_i^{-1}\right)\chi_{\overline{\Gamma}_\mu}(S) \\
&= \sum_{i=1}^n \sum_{S \text{ in } T_i^{-1}\mathfrak{H}T_i} \chi_{\Delta_\nu}\left(T_iST_i^{-1}\right)\chi_{\overline{\Gamma}_\mu}(T_iST_i^{-1}) \\
&= \sum_{i=1}^n \sum_{R \text{ in } \mathfrak{H}} \chi_{\Delta_\nu}(R)\chi_{\overline{\Gamma}_\mu}(R) = n \sum_{R \text{ in } \mathfrak{H}} \chi_{\Delta_\nu}(R)\chi_{\Delta_{\overline{\Gamma}_\mu}}(R).
\end{aligned}$$

Nun ist offenbar $\Delta_{\overline{\Gamma}_\mu} = \overline{\Delta}_{\Gamma_\mu}$, also die letzte Summe

$$\sum_{R \text{ in } \mathfrak{H}} \chi_{\Delta_\nu}(R)\chi_{\overline{\Delta}_{\Gamma_\mu}}(R) = h \cdot k'_{\mu\nu}$$

wenn $k'_{\mu\nu}$ angibt, wie oft Δ_ν in Δ_{Γ_μ} enthalten. So folgt III, 56

$$\begin{aligned} gk_{\mu\nu} &= nhk'_{\mu\nu} \\ k_{\mu\nu} &= k'_{\mu\nu} \end{aligned}$$

w. z. b. w.

3.9 Der Basissatz für Abelsche Gruppen. (12.Juli 1924)

Schreier's proof that every finitely generated abelian group is isomorphic to the direct product of finitely many cyclic groups, each being either finite of prime power order or infinite.

III, 57

12. Juli 1924.

(Beweis von Dr. Schreier, Hamburg).

Es sei $\mathfrak{G}$ eine Abelsche Gruppe von endlich oder unendlich vielen Elementen, die aus endlich vielen Elementen $A_1, \dots, A_n$ erzeugt werden kann. Es sei ferner ein vollständiges System von Relationen gegeben (bei endlichen Gruppen genügt die Gruppentafel, sonst möglicherweise unendlich viele), aus denen alle anderen Folgen sind. Diese Relationen haben sämtlich die Form

$$A_1^{a_{i1}} \cdots A_n^{a_{in}} = E\,; \quad i = 1, 2, \dots$$

und definieren eine n spaltige Matrix

$$A = (a_{ik})\,; \quad \begin{pmatrix} i = 1, 2, \dots \\ k = 1, 2, \dots\; n \end{pmatrix}$$

In dieser Matrix A darf offenbar jede Zeilen– und Spaltenvertauschung ausgeführt werden, da sie nur auf Vertauschung der Relationen oder Vertauschung der Produktreihenfolge hinausläuft. Letzteres ist erlaubt, weil $\mathfrak{G}$ Abelsch ist.

Ferner dürfen die Operationen: Addition einer Zeile zu einer anderen und entsprechend für die Spalten, sowie dasselbe mit Subtraktion, also auch mit beliebigen ganzen Faktoren, ausgeführt werden. Denn das bedeutet nur Übergang zu einem äquivalenten Relationensystem bezw. zu einem äquivalenten Erzeugenden–System.

Man kann also alle „elementaren“ Transformationen ausführen, und so die Matrix A in die Normalform

$$A_0 = \begin{pmatrix} a_1 & & & \\ & a_2 & & \\ & & \ddots & \\ & & & a_n \end{pmatrix}$$

transformieren ($PAQ = A_0$). Das bedeutet also, daß man Relationen und Erzeugende so transformieren kann, daß A_0 die Relationen–Matrix wird. Die neuen Erzeugenden seien $S_1, \dots, S_n$. Dann lauten die neuen Relationen III, 58

$$S_1^{a_1} = E, \; \dots \; , S_n^{a_n} = E.$$

Ist hierin ein $a_i = 0$, so kommt S_i in den Relationen nicht vor, hat also die Ordnung ∞. Ist $a_i = 1$, so ist $S_i = E$, kann also fortgelassen werden. Die $a_i > 1$ liefern Elemente der endlichen Ordnung a_i. Die allgemeinste Relation lautet jetzt, nachdem die $S_i = E$ fortgelassen und die von der unendlichen Ordnung an den Schluß gestellt sind, wenn $S_1, \dots, S_m$ endliche Ordnung haben:

$$S_1^{c_1 a_1} \dots S_m^{c_m a_m} = E$$

Die Faktorgruppe des Relationen–Normalteilers (s. S. 3]) in der freien Gruppe von $S_1, \dots, S_n$ („Abelschen" freien Gruppe) wird dann durch

$$S_1^{x_1} \dots S_m^{x_m} S_{m+1}^{x_{m+1}} \dots S_n^{x_n}\,; \quad (x_1, \dots, x_m \mod a_1, \dots, a_m)$$

repräsentiert, in eindeutiger Darstellung, d. h. jedes Gruppenelement läßt sich eindeutig auf diese Form bringen.

Will man noch die Elemente der Basis in solche von Primzahlpotenzordnung aufspalten, so behandle man ein S der Ordnung

$$a = p_1^{\nu_1} \cdots p_r^{\nu_r} = p_1^{\nu_1} Q_1 = p_2^{\nu_2} Q_2 = \cdots$$

so, daß man

$$S^{Q_1}, \dots, S^{Q_r}$$

für S einführt.

Die Invarianz der vorkommenden p^ν folgt aus der Invarianz der zahlentheoretischen Elementarteiler der Matrix A bei Transformation. Die Elementarteiler für p sind eben die Gesamtheit der in den a_i steckenden Potenzen von p.

3.10 Theorie der hyperkomplexen Zahlen. (Juli 1924)

On hypercomplex numbers and their matrix representations, following Frobenius [Fro03].

III, 59

Juli 1924.

(Nach Frobenius, Berl. Ber. 1903)

Es seien $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ n Rechenzeichen, von denen beliebige lineare Kombinationen

$$\alpha = \sum_i a_i \varepsilon_i,$$

mit Koeffizienten (aus irgendeinem Integritätsbereich oder im Sinne der späteren Anwendungen besser gleich) aus irgendeinem Körper, nach den Regeln der gewöhnlichen Addition gebildet werden mögen. Ferner werde den ε_i der Charakter der linearen Unabhängigkeit verliehen, d. h. zwei solche Größen

$$\alpha = \sum_i a_i \varepsilon_i\,; \quad \beta = \sum_i b_i \varepsilon_i$$

dann und nur dann gleich genannt, wenn alle ihre „Koordinaten" übereinstimmen, d. h.

$$a_i = b_i\,, \quad \text{kurz } a = b$$

ist.

Für die Produkte der ε_i werde das Bestehen der folgenden Formeln festgesetzt:

$$\varepsilon_i \varepsilon_k = \sum_\ell a_{ik\ell} \varepsilon_\ell,$$

wo die $a_{ik\ell}$ wieder Elemente des Koeffizientenkörpers sind. Damit ist für irgendzwei „hyperkomplexe Größen"

$$\alpha = \sum_i a_i \varepsilon_i\,; \quad \beta = \sum_i b_i \varepsilon_i$$

ihr Produkt eindeutig definiert zu

$$\alpha\beta = \gamma = \sum_i c_i \varepsilon_i = \sum_i \varepsilon_i \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda b_\mu,$$

d. h.

$$c_i = \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda b_\mu \tag{1}$$

Man kann das alles auch ohne Benutzung der ε_i ausdrücken, als einen Formalismus, nach dem beliebige Vektoren $a = (a_i)$, $b = (b_i)$ aus dem Koeffizientenkörper zu einem bestimmten neuen Vektor $c = (c_i)$ zusammenzusetzen sind. III, 60

Fordert man für diese Komposition das assoziative Gesetz, so kommt das auf das Bestehen der n^4 Gleichungen:

$$\sum_\ell a_{ik\ell} a_{\ell\mu\nu} = \sum_\ell a_{i\ell\nu} a_{k\mu\ell} \tag{2}$$

zwischen den Koeffizienten der dreidimensionalen „Kompositionsmatrix“ $A = (a_{ik\ell})$ hinaus.

Diese Relationen mögen vorausgesetzt werden. Dann gilt stets

$$(\alpha\beta)\gamma = \alpha(\beta\gamma),$$

d. h. die definierte Komposition ist assoziativ. Daß das distributive Gesetz der Addition und Multiplikation gilt, ist klar. Denn man hat:

$$\begin{aligned} \alpha(\beta+\gamma) &= \sum_i \varepsilon_i \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda (b_\mu + c_\mu) \\ \alpha\beta + \alpha\gamma &= \sum_i \varepsilon_i \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda b_\mu + \sum_i \varepsilon_i \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda c_\mu . \end{aligned}$$

Wir haben dann:

III, 61

Satz 1. *Es sei k ein beliebiger Körper. Im Bereiche der n–komponentigen Vektoren $a = (a_i)$, $b = (b_i)$, ... dieses Körpers sei außer der in elementarer Weise (komponentenweise) erklärten Addition und Zahlmultiplikation von Vektoren die Komposition zweier Vektoren allgemein durch*

$$(1.) \qquad ab = c\,, \quad \text{wo } c_i = \sum_{\lambda,\mu} a_{\lambda\mu i} a_\lambda b_\mu$$

erklärt, wo die dreidimensionale Matrix $A = (a_{ik\ell})$ aus k irgendeine den Bedingungen

$$(2.) \qquad \sum_\ell a_{ik\ell} a_{\ell\mu\nu} = \sum_\ell a_{i\ell\nu} a_{k\mu\ell}$$

unterworfene Matrix ist. Dann besteht für diese Komposition das assoziative und distributive Gesetz. Faßt man die Vektoren durch Einführung von n Rechenzeichen $\varepsilon_1, \ldots, \varepsilon_n$ gemäß

$$\alpha = \sum_i a_i \varepsilon_i$$

zu neuen Rechenzeichen zusammen, mit der Festsetzung, daß

$$\alpha = \beta \quad \text{dann und nur dann, wenn} \quad a = b,$$

so kann man immer die Vektoren a durch die zugeordneten α und umgekehrt ersetzen, wenn man mit den α nach den elementaren Additionsregeln und nach den Formeln

$$(3.) \qquad \varepsilon_i \varepsilon_k = \sum_\ell a_{ik\ell} \varepsilon_\ell$$

rechnet. Der so definierte Bereich $\mathfrak{A}$ heißt ein Bereich hyperkomplexer Größen über k.

Definition 1: *Ein System von Matrizen A_a, das den hyperkomplexen Größen $a = (a_i)$ eindeutig zugeordnet ist, heißt eine Darstellung des Bereiches $\mathfrak{A}$, wenn für beliebige a, b aus ihm*

$$A_a + A_b = A_{a+b}$$
$$A_a . A_b = A_{ab}$$

gilt. Ist dann

$$\varphi(a, b, \ldots) = 0 \tag{4.}$$

eine beliebige ganz rationale Gleichung mit Koeffizienten aus k zwischen den hyperkomplexen Größen, so gilt auch

$$\varphi(A_a, A_b, \ldots) = 0. \tag{5.}$$

Ist die Zuordnung gegenseitig eindeutig, so heißt die Darstellung einstufig isomorph. Dies ist dann und nur dann der Fall, wenn außer $A_0 = 0$ keine Matrix A_a verschwindet. In diesem Falle folgt auch umgekehrt (4.) *aus* (5.)

Beweis: Es ist nach den Zuordnungsgesetzen III, 62

$$0 = A_0 = A_{\varphi(a,b,\ldots)} = \varphi(A_a, A_b, \ldots).$$

Daß $A_0 = 0$, folgt unmittelbar aus

$$A_0 + A_0 = A_{0+0} = A_0.$$

Ist ferner die Zuordnung gegenseitig eindeutig, so ist einzig und allein $A_0 = 0$. Aber auch umgekehrt, wenn nur $A_0 = 0$ ist, ist die Zuordnung gegenseitig eindeutig. Denn wäre dann

$$A_a = A_b\,, \quad \text{d.h. } A_{a-b} = 0,$$

so folgte $a - b = 0$, $a = b$. In diesem Falle folgt dann (4.) aus (5.)

$$0 = \varphi(A_a, A_b, \ldots) = A_{\varphi(a,b,\ldots)}\,, \quad \text{also} \quad \varphi(a, b, \ldots) = 0.$$

Satz 2. *Es bezeichne allgemein*

$$A_\lambda = (a_{i\lambda k})\,; \qquad \begin{pmatrix} i \text{ Zeilen} \\ k \text{ Spalten} \end{pmatrix}$$

die Matrix, die aus A durch Festhalten des mittleren Index λ entsteht, und es werde

$$A_a = \sum_\lambda A_\lambda a_\lambda \quad \textit{für} \quad a = (a_\lambda)$$

gesetzt. Dann bilden die A_a eine Darstellung, die sogenannte reguläre Darstellung von $\mathfrak{A}$.

Beweis: $A_a + A_b = A_{a+b}$ ist nach Definition klar. Ferner ist

$$\begin{aligned} A_{ab} &= \sum_\ell A_\ell \sum_{\lambda,\mu} a_{\lambda\mu\ell} a_\lambda b_\mu = \left(\sum_{\lambda,\mu} a_\lambda b_\mu \sum_\ell a_{i\ell k} a_{\lambda\mu\ell} \right) \\ &= \left(\sum_{\lambda,\mu} a_\lambda b_\mu \sum_\ell a_{i\lambda\ell} a_{\ell\mu k} \right) = \left(\sum_\ell \sum_\lambda a_{i\lambda\ell} a_\lambda \cdot \sum_\mu a_{\ell\mu k} b_\mu \right) = A_a A_b. \end{aligned}$$

Definition 2. *Der durch Vertauschung der ersten beiden Indizes von A entstehende Bereich $\mathfrak{B}$ heißt zu dem ursprünglichen $\mathfrak{A}$ antistroph. Diese Beziehung ist gegenseitig. Die Koordinaten von ab im antistrophen Bereich sind die von ba im ursprünglichen und umgekehrt.*

III, 63 **Satz 3.** *Es sei allgemein*

$$B_\lambda = (a_{\lambda ik})\,; \qquad \begin{pmatrix} i \text{ Zeilen} \\ k \text{ Spalten} \end{pmatrix}$$

und es werde

$$B_a = \sum_\lambda B_\lambda a_\lambda \quad \textit{für} \quad a = (a_\lambda)$$

gesetzt. Dann bilden die B_a eine Darstellung des antistrophen Bereichs $\mathfrak{B}$, die auch die antistrophe Darstellung von $\mathfrak{A}$ heißt.

Beweis: Die B_a sind offenbar die reguläre Darstellung des Bereichs $\mathfrak{B}$ nach Definition desselben. Auf Grund der Beziehung beider Bereiche (Definition 2)

folgt noch:

Satz 4. *Es gilt allgemein* $B_a + B_b = B_{a+b}\,;\ B_a \cdot B_b = B_{ba}$.

Satz 5. *Die Matrizen der regulären Darstellung von* $\mathfrak{A}$ *sind mit denen der antistrophen* (*regulärer von* $\mathfrak{B}$) *vertauschbar*:

$$A_a B_b = B_b A_a.$$

Für die Matrizen

$$C_\lambda = (a_{ik\lambda})\,;\ \begin{pmatrix} i \text{ Zeilen} \\ k \text{ Spalten} \end{pmatrix};\ C_\lambda = \sum_\lambda C_\lambda a_\lambda\,;\ a = (a_\lambda),$$

die die parastrophe Darstellung von $\mathfrak{A}$ *heißen, gilt die Kompositionsregel*:

$$A_a C_b = C_b B'_a.$$

Beweis: Diese Kompositionsformeln brauchen offenbar nur für die A_λ, B_λ, C_λ bewiesen zu werden. Dann sind sie aber identisch mit dem Assoziativ–Gesetz (2.) in Satz 1.

Natürlich ist die Bezeichnung antistrophe und parastrophe „Darstellung" nicht direkt zu verstehen, denn die parastrophen Matrizen C_a sind weder Darstellungen im Sinne der Definition 1 von $\mathfrak{A}$ noch von $\mathfrak{B}$, und die antistrophen zwar an $\mathfrak{B}$ aber nicht von $\mathfrak{A}$.

Satz 6. *Ist* $|A_a| \neq 0$, *so ist die Gleichung* III, 64

$$xa = b$$

für jedes b *aus* $\mathfrak{A}$ *eindeutig lösbar, ebenso, falls* $|B_a| \neq 0$, *die Gleichung*

$$ax = b.$$

Beweis: Die Lösung dieser Gleichungen erfordert nach (1.) in Satz 1 die Auflösung eines linearen Gleichungssystems mit Determinante $|A_a|$ bezw. $|B_a|$.

Satz 7. *Existiert in $\mathfrak{A}$ ein p, für das*

$$|A_p| \neq 0\,, \quad |B_p| \neq 0,$$

so gibt es in $\mathfrak{A}$ (also auch in $\mathfrak{B}$) ein e, für das

$$ae = ea = a$$

für jedes a aus $\mathfrak{A}$ gilt. Dies e ist eindeutig bestimmt, und heißt Haupteinheit von $\mathfrak{A}$ (und $\mathfrak{B}$). Es gilt dann

$$A_e = B_e = E.$$

Beweis: Nach Satz 6 existiert ein e, sodaß

$$ep = p$$

und ein e', sodaß

$$pe' = p$$

ist. Ferner existiert zu jedem a ein q sodaß

$$pq = a$$

und ein r, sodaß

$$rp = a$$

ist. Für jedes a folgt dann:

$$\begin{aligned} epq = pq, &\quad \text{d. h.} \quad ea = a \\ rpe' = rp, &\quad \text{d. h.} \quad ae' = a \end{aligned}$$

Danach ist speziell

$$ee' = e = e'.$$

e ist nach Satz 6 eindeutig bestimmt. Die Eindeutigkeit folgt natürlich auch aus der bewiesenen Eigenschaft $ae = ea = a$ für jedes a. Aus

III, 65

$$\begin{aligned} A_e \cdot A_p &= A_{ep} = A_p \\ B_e \cdot B_p &= B_{pe} = B_p \end{aligned}$$

folgt dann durch hintere Multiplikation mit A_p^{-1}, B_p^{-1}, daß

$$A_e = B_e = E$$

sein muß.

Satz 8. *Die Voraussetzungen von Satz 7 sind sicher realisiert, wenn nur die Existenz eines p mit $|C_p| \neq 0$ feststeht.*

Beweis: Sei $|C_p| \neq 0$. Dann hat das System

$$\sum_k \left(\sum_\lambda a_{ik\lambda} p_\lambda \right) e_k = p_i,$$

d. h. die p_i sind Lösung eines Gleichungssystems mit der Matrix $A_e - E$. Wir bilden nun

$$\begin{aligned} A_e C'_p &= \left(\sum_\nu a_{i\nu k} e_\nu \right) \left(\sum_\lambda a_{ki\lambda} p_\lambda \right) = \left(\sum_{\nu,\lambda} e_\nu p_\lambda \sum_\ell a_{i\nu\ell} c_{k\ell\lambda} \right) \\ &= \left(\sum_{\nu,\lambda,\ell} e_\nu p_\lambda a_{\ell\nu\lambda} a_{ki\ell} \right) = \left(\sum_\ell a_{ki\ell} p_\ell \right) = C'_p \end{aligned}$$

Durch Multiplikation mit ${C'}_p^{-1}$ folgt also:

$$A_e = E.$$

Auf ähnlichem Wege, oder aus Satz 6:

$$C_p = A_e C_p = C_p B'_e$$

folgt dann auch

$$B_e = E.$$

Es erfüllt also $p = e$ die Voraussetzungen des Satzes 7 und ist offenbar gleichzeitig das Element e, das dann nach Satz 7 existiert $\big((1.), \text{Satz } 1\big)$. III, 66

Satz 9. *Bestehen die Voraussetzungen von Satz 7, so sind die Darstellungen $\{A_a\}$ von $\mathfrak{A}$ und $\{B_a\}$ von $\mathfrak{B}$ einstufig, d. h. aus*

$$A_a = A_b \quad \textit{oder} \quad B_a = B_b$$

folgt

$$a = b.$$

Die Matrizen A_λ und die Matrizen B_λ sind linear unabhängig.

Beweis: Wäre für ein $a \neq 0$: $A_a = 0$, so folgte

$$\sum_{\lambda,i} a_{i\lambda k} a_\lambda e_i = 0,$$

also

$$a = ea = 0.$$

Genau ebenso folgt aus $B_a = 0$, daß $a = 0$ sein muß. Das genügt zur Einstufigkeit von $\{A_a\}$ und $\{B_a\}$.

Satz 10. *Auch aus jeder der Gleichungen:*

$$A_e = B_b, \; C_a = C_b, \; C'_a = C_b$$

folgt

$$a = b.$$

wenn die Voraussetzungen von Satz 7 gelten.

Beweis: Die Relationen $A_e = B_e = E$ sagen ausführlich

$$\begin{aligned} \sum_\lambda a_{i\lambda k} e_\lambda &= e_{ik} \\ \sum_\lambda a_{\lambda ik} e_\lambda &= e_{ik}. \end{aligned}$$

Sei nun $A_a = B_b$, also

$$\sum_\lambda a_{i\lambda k} a_\lambda = \sum_\lambda a_{\lambda ik} b_\lambda$$

so folgt für jedes k

$$\begin{aligned} \sum_{\lambda,i} a_{i\lambda k} a_\lambda e_i &= \sum_{\lambda,i} a_{\lambda ik} b_\lambda e_i \\ \sum_\lambda a_\lambda e_{\lambda k} &= \sum_\lambda b_\lambda e_{\lambda k} \\ a_k &= b_k. \end{aligned}$$

III, 67 Ebenso folgt aus $C_a = C_b$:

$$\sum_{\lambda} a_{ik\lambda} a_{\lambda} = \sum_{\lambda} a_{ik\lambda} b_{\lambda}$$

für jedes k

$$\begin{aligned} \sum_{i,\lambda} a_{ik\lambda} a_{\lambda} e_i &= \sum_{i,\lambda} a_{ik\lambda} b_{\lambda} e_i \\ \sum_{\lambda} a_{\lambda} e_{k\lambda} &= \sum_{\lambda} b_{\lambda} e_{k\lambda} \\ a_k &= b_k. \end{aligned}$$

Genau ebenso schließt man für $C_a = C'_b$.

Satz 11. *Unter den Voraussetzungen von Satz 7 gilt: Ist U mit allen A_a vertauschbar, so ist U ein B_b. Ist U mit allen B_a vertauschbar, so ist U ein A_b.*

Beweis: Es genügt nach Definition 2, dies für die A_a zu zeigen. Sei also für $U = (u_{ik})$:

$$UA_a = A_a U,$$

d. h.

$$\sum_{\lambda,\ell} a_{\ell\lambda k} a_{\lambda} u_{i\ell} = \sum_{\lambda,\ell} a_{i\lambda\ell} a_{\lambda} u_{\ell k},$$

so folgt, wenn

$$\sum_{i} u_{ik} e_i = b_k$$

gesetzt wird,

$$\begin{aligned} \sum_{\lambda,\ell} a_{\ell\lambda k} a_{\lambda} b_{\ell} &= \sum_{\lambda,\ell,i} a_{i\lambda\ell} e_i a_{\lambda} u_{\ell k} \\ &= \sum_{\lambda,\ell} e_{\lambda\ell} a_{\lambda} u_{\ell k} \\ &= \sum_{\lambda} a_{\lambda} u_{\lambda k}, \end{aligned}$$

und da dies für alle a gilt,

$$\begin{aligned} u_{\lambda k} &= \sum_{\ell} a_{\ell\lambda k} b_{\ell} \\ U &= B_b. \end{aligned}$$

III, 68

Satz 12. $\mathfrak{A}$ *und* $\mathfrak{B}$ *heißen dann und nur dann Systeme hyperkomplexer Zahlen mit Haupteinheit, wenn ein* e *existiert, für das*

$$A_e = B_e = E$$

ist.

Ist dies der Fall, so sind die Voraussetzungen von Satz 7 erfüllt, und es ist e *die eindeutig bestimmte Größe, für die*

$$ae = ea = a \quad \text{für jedes} \quad a$$

gilt. Sind umgekehrt die Voraussetzungen von Satz 7 (oder, was dasselbe bedeutet, auch nur die von Satz 8) erfüllt, so sind $\mathfrak{A}$, $\mathfrak{B}$ *Systeme hyperkomplexer Zahlen mit Haupteinheit.*

Für Systeme mit Haupteinheit gelten Satz 9—11.

Beweis: Ist $A_e = B_e = E$, so sind natürlich die Voraussetzungen von Satz 7 für $p = e$ erfüllt. Daß dann e die eindeutig bestimmte Haupteinheit ist, folgt aus dem ja dann gültigen Satz 9, oder aus den Multiplikationsformeln (1.) von Satz 1, die ja lehren, daß dann e den Bedingungen $ae = ea = a$ für jedes a genügt.

Der Rest des Satzes ist nach Satz 7 klar.

Wir beschränken uns fortan auf Systeme $\mathfrak{A}$, $\mathfrak{B}$ mit Haupteinheit e.

3.11 Eine Knoppsche Frage aus der elementaren Zahlentheorie. (Nov. 1924)

A problem by Knopp from elementary number theory. It appears that Hasse was not satisfied with his solution which in the end requires factorisation of many numbers. Therefore he later posed (jointly with I. Schur) this problem as a question in the "Jahresbericht der Deutschen Mathematiker-Vereinigung", vol.36 (1927) p.38. A solution of that question was then given jointly by A. Brauer and R. Brauer and published in the same volume, p.90. That solution runs essentially on the same lines as here but it required finding the representation of numbers by certain quadratic forms instead of factorising. We do not know whether Hasse was more satisfied with the Brauer solution. Hasse refers to a letter by R. Schmidt of 21 November 1924. We did not find this letter among the Hasse papers.

III, 69

November 1924

(Angeregt durch Brief v. R. Schmidt v. 21. XI. 24).

Für welche natürlichen Zahlen x, y sind

$$\frac{x^2+m}{y} \quad \text{und} \quad \frac{y^2+m}{x} \quad \text{ganz,}$$

wobei $m \geqq 1$ eine natürliche Zahl ist, und (x, y) relativ prim.

Man erkennt sofort, daß jede Lösung (x_n, x_{n+1}) eine ganze Lösungskette

$$\ldots, x_{n-2}, x_{n-1}, x_n, x_{n+1}, x_{n+2}, \ldots$$

die beiderseits ins Unendliche erstreckt ist, nach sich zieht, derart daß jedes benachbarte Paar Lösung ist, und die Formeln gelten

$$x_n^2 + m = x_{n-1}x_{n+1}\,; \quad (n = -\infty \ldots + \infty).$$

und zeigt dann, daß diese Kette den Ungleichungen

(a) $\quad \cdots > x_{-2} > x_{-1} > x_0 < x_1 < x_2 < \cdots$

oder

(b) $\quad \cdots > x_{-2} > x_{-1} > x_0 = 1 = x_1 < x_2 < x_3 < \cdots$

genügt, wenn der Nullpunkt geeignet gewählt wird. Dabei stellt sich im Falle (a) noch

$$x_1 < m$$
$$x_{-1} < m$$

heraus, wenn $m > 1$ (für $m = 1$ liegt notwendig Fall (b) vor)

Wenn es nun gelungen ist, alle reduzierten Lösungen zu finden, d. h. im Falle $m = 1$ die Lösung $(1, 1)$, im Falle $m > 1$ alle Lösungen mit $1 \leqq x, y < m$,
III, 70 was stets durch endlich viele Versuche erreicht werden kann, so ergeben sich aus ihnen *alle* Lösungen durch Bildung der zugehörigen Ketten, wobei auch mehrere reduzierte Lösungen derselben Kette angehören können, wie z. B. für $m = 11$ in der Kette

$$\ldots, 18, \underline{5}, \underline{2}, \underline{3}, \underline{10}, \ldots$$

wo im rechten Zweig die beiden Lösungen $2, 3$ und $3, 10$ reduziert sind.

Jede Kette hat die Größe

$$k = \frac{x_n^2 + x_{n+1}^2 + m}{x_n x_{n+1}} = \frac{x_{n-1} + x_{n+1}}{x_n},$$

die sich als ganze Zahl $\geqq 3$ erweist, zur Invariante, und genügt dann der linearen, homogenen Differenzengleichung 2. Ordnung

$$x_{n+2} = k x_{n+1} - x_n.$$

Nach dem bekannten Auflösungsschema hierfür resultiert so die Darstellung

$$x_n = \frac{y - \varepsilon' x}{\varepsilon - \varepsilon'} \varepsilon^n - \frac{y - \varepsilon x}{\varepsilon - \varepsilon'} \varepsilon'^n; \quad (n = -\infty \ldots + \infty)$$

für die Kette, wenn (nicht notwendig wie oben in (a) und (b)) das beliebige, benachbarte Paar x, y als x_0, x_1 bezeichnet ist.

Dabei bedeuten $\varepsilon, \varepsilon'$ in irgendeiner Reihenfolge die Wurzeln der quadratischen Gleichung

$$x^2 - kx + 1 = 0,$$

also Einheiten mit $n(\varepsilon) = +1$ des reell–quadratischen Körpers $R(\sqrt{k^2 - 4})$, dessen Diskriminante kein Quadrat sein kann ($k \geqq 3$). Die Lösung läßt sich dann
III, 71 unter Verwendung des Zeichens $\delta(\alpha)$ für die Differente $\alpha - \alpha'$ der Zahl α in

$R(\sqrt{k^2-4})$ auch in der Form:

$$x_n = \frac{y\delta(\varepsilon^n) - x\delta(\varepsilon^{n-1})}{\delta(\varepsilon)}\,; \quad (n = -\infty \ldots + \infty)$$

schreiben.

ε ist die niedrigste Einheit der Diskriminante k^2-4 mit $n(\varepsilon) = +1$, d. h. die kleinste positive Lösung von

$$u^2 - (k^2-4)v^2 = 4.$$

Falls k^2-4 quadratfrei, bezw. $\frac{k^2-4}{4}$ quadratfrei ist, also die Grundeinheit des Strahles der Körperzahlen mit $n(\alpha) > 0$, sonst, wenn

$$k^2 - 4 = \ell^2 d$$

und d die Körperdiskriminante ist, die Grundeinheit des Strahles:

$$\begin{aligned}&\alpha \equiv \text{rat. zu } \ell \text{ prime Zahl mod. } \ell\\ &n(\alpha) > 0.\end{aligned}$$

Für den Typus (b) ist die Kette symmetrisch und von der Form

$$\ldots, m+1, 1, 1, m+1, \ldots$$

Im Falle (a) kann Symmetrie eintreten, wenn nämlich

$$x_{-1} = x_1$$

also

$$x_0^2 + m = x_1^2, \quad x_1^2 + m = x_0 x_2,$$

und dies findet dann und nur dann statt, wenn

$$\begin{aligned}m+1 &= \ell^2\\ \text{oder}\quad m+4 &= \ell^2\end{aligned}$$

ein Quadrat ist. Sonst sind die beiderseitigen Lösungen alle verschieden. Zur Aufstellung der reduzierten Lösungen für $m > 1$ zerlege man die $\varphi(m)$ Zahlen III, 72

$$x_0^2 + m, \quad \text{wo} \quad x_0 < m, \ (x_0, m) = 1$$

auf alle möglichen Arten in Faktoren

$$x_0^2 + m = x_{-1}x_{+1}\,; \quad (1 \leqq x_1 \leqq \sqrt{x_0^2 + m})$$

und prüfe, ob

$$x_1^2 + m \equiv 0 \mod x_0$$

ist. Dann und nur dann, wenn dies der Fall ist, liefern x_0, x_1 eine Kette.

Im Falle, daß die Lösungen x, y nicht mehr untereinander u. somit zu m prim vorausgesetzt werden, werden die Untersuchungen modifiziert. Vermutlich kommt man mit ähnlichen Methoden durch.

3.12 Zur Theorie der verallgemeinerten Kummerschen Körper. (20.12.1924)

Kummer theory for prime power exponents.

III, 73

20. XII. 1924

Satz 1. *Es enthalte k die ℓ^ν–ten Einheitswurzeln (ℓ Primzahl, $\nu \geqq 1$) und es sei α eine Zahl aus k, die nicht ℓ–te Potenz in k ist. Dann ist $k(\sqrt[\ell^\nu]{\alpha})$ zyklisch vom Relativgrad ℓ^ν über k.*

Beweis: Es ist nur zu zeigen, daß $k(\sqrt[\ell^\nu]{\alpha})$ den Rel. Grad ℓ^ν hat, d. h. daß $x^{\ell^\nu} - \alpha$ in k irreduzibel ist. Wäre nun ein Faktor m–ten Grades vorhanden, so wäre sein absolutes Glied als Produkt der Konjugierten $\sqrt[\ell^\nu]{\alpha}, \zeta_\nu \sqrt[\ell^\nu]{\alpha}, \ldots$, wo ζ_ν eine primitive ℓ^ν–te Einheitswurzel ist, von der Form

$$\zeta_\nu^k \left(\sqrt[\ell^\nu]{\alpha}\right)^m = \gamma \quad \text{in } k$$

Es folgte also

$$\alpha^m = \gamma^{\ell^\nu}.$$

Hier muß $m = m_1\ell$ sein, da sonst α eine ℓ–te Potenz in k wäre, und da die ℓ–ten Einheitswurzeln selbst $\ell^{\nu-1}$–te Potenzen in k sind, folgt

$$\alpha^{m_1} = \gamma_1^{\ell^{\nu-1}}$$

Daraus weiter: $m_1 = m_2\ell$ und

$$\begin{array}{rcl} \alpha^{m_2} & = & \gamma_2^{\ell^{\nu-2}} \\ \multicolumn{3}{c}{\dotfill} \\ \alpha^{m_{\nu-1}} & = & \gamma_{\nu-1}^{\ell} \end{array}$$

und $m_{\nu-1} = m_\nu \ell$, also $m = m_\nu \ell^\nu$. Daher kann kein irreduzibler Faktor niedrigeren als ℓ^ν–ten Grades von $x^{\ell^\nu} - \alpha$ in k existieren, w. z. b. w.

Zusatz. *Enthält k als höchste die ℓ^ϱ–ten E. W. ($0 \leqq \varrho < \nu$), so folgt nur, daß $k(\sqrt[\ell^\nu]{\alpha})$ entweder den Grad ℓ^ν hat, oder $\alpha = \gamma^\ell \cdot \zeta^x$ ist, wo ζ eine ℓ^ϱ–te Einheitswurzel ist.*

III, 74 **Satz 2.** *Es enthalte k die ℓ^ν–ten und ℓ^μ–ten Einheitswurzeln ($\nu, \mu \geqq 1$), und es seien α, β keine ℓ–ten Potenzen in k. Dann folgt aus*

$$k\left(\sqrt[\ell^\mu]{\beta}\right) \prec k\left(\sqrt[\ell^\nu]{\alpha}\right),$$

daß $\mu \leqq \nu$ und

$$\beta = \alpha^x \gamma^{\ell^\mu}; \quad x \not\equiv 0 \text{ mod. } \ell,\ \gamma \text{ in } k$$

ist.

Beweis: $k\left(\sqrt[\ell^\mu]{\beta}\right)$ ist als Teilkörper des rel. zyklischen $k\left(\sqrt[\ell^\nu]{\alpha}\right)$ über k mit dem einzigen Unterkörper gleichen, nämlich ℓ^μ–ten Grades $k\left(\sqrt[\ell^\mu]{\alpha}\right)$ identisch:

$$k\left(\sqrt[\ell^\mu]{\beta}\right) = k\left(\sqrt[\ell^\mu]{\alpha}\right).$$

Daher ist auch $\mu \leqq \nu$, weil $k\left(\sqrt[\ell^\mu]{\beta}\right)$ sonst kein Teilkörper wäre. Führt man die erzeugende Substitution $\left(\sqrt[\ell^\mu]{\alpha} : \zeta_\mu \sqrt[\ell^\mu]{\alpha}\right)$ von $k\left(\sqrt[\ell^\mu]{\alpha}\right)$ aus, so muß auch $\sqrt[\ell^\mu]{\beta}$ in eine konjugierte $\zeta_\mu^x \sqrt[\ell^\mu]{\beta}$ übergehen. In der Darstellungsgleichung

$$\sqrt[\ell^\mu]{\beta} = \sum_{i=0}^{\ell^\mu - 1} \gamma_i \left(\sqrt[\ell^\mu]{\alpha}\right)^i; \quad \gamma_i \text{ in } k$$

gibt das

$$\zeta_\mu^x \sqrt[\ell^\mu]{\beta} = \sum_i \gamma_i \zeta_\mu^x \left(\sqrt[\ell^\mu]{\alpha}\right)^i = \sum_i \gamma_i \zeta_\mu^i \left(\sqrt[\ell^\mu]{\alpha}\right)^i,$$

also wegen der Eindeutigkeit (Grad ist ℓ^μ):

$$\gamma_i = 0 \quad \text{für } i \neq x,$$

d. h.

$$\sqrt[\ell^\mu]{\beta} = \gamma_x \left(\sqrt[\ell^\mu]{\alpha}\right)^x$$
$$\beta = \alpha^x \gamma_x^{\ell^\mu}$$

Da β keine ℓ–te Potenz in k ist, muß $x \not\equiv 0$ mod. ℓ sein.

Satz 3. *k enthalte die ℓ^ν–ten Einheitswurzeln, und es sei* III, 75

$$1 \leqq \mu, \nu_1, \ldots, \nu_s \leqq \nu.$$

Ferner seien $\alpha_1, \ldots, \alpha_s$ unabhängig in Bezug auf ℓ–te Potenzen und β keine ℓ–te Potenz in k. Wenn dann

$$k\left(\sqrt[\ell^\mu]{\beta}\right) \prec k\left(\sqrt[\ell^{\nu_1}]{\alpha_1}, \ldots, \sqrt[\ell^{\nu_s}]{\alpha_s}\right)$$

ist, besteht eine Relation

$$\beta = \alpha_1^{x_1} \ldots \alpha_s^{x_s} \gamma^{\ell^\mu},$$

wo $x_1, \ldots, x_s$ nicht sämtlich $\equiv 0 \bmod. \ell$ sind, und γ eine Zahl aus k ist.

Beweis: Für $s = 1$ ist das in Satz 2 bewiesen. Es sei richtig bis $s-1$. Wenn dann $k\left(\sqrt[\ell^\mu]{\beta}\right)$ schon in

$$K = k\left(\sqrt[\ell^{\nu_1}]{\alpha_1}, \ldots, \sqrt[\ell^{\nu_{s-1}}]{\alpha_{s-1}}\right)$$

enthalten ist, besteht eine solche Relation. Sei das also nicht der Fall. Wäre nun $\sqrt[\ell^\mu]{\alpha_s}$ mit $1 \leqq p \leqq \nu_s$ schon in K enthalten, so folgte aus demselben Grunde eine Relation

$$\alpha_s = \alpha_1^{x_1} \cdots \alpha_{s-1}^{x_{s-1}} \gamma^{\ell^p}; \quad p \geqq 1,$$

die nach Voraussetzung über $\alpha_1, \ldots, \alpha_s$ unmöglich ist. Also ist $K\left(\sqrt[\ell^{\nu_s}]{\alpha_s}\,^\nu\right)$ vom Grade ℓ^{ν_s} über K. (Es genügt nach Satz 1 natürlich schon dieser Schluß für $p = 1$). Da $K\left(\sqrt[\ell^\mu]{\beta}\right)$ darin enthalten ist, ist nach Satz 2*)

$$\sqrt[\ell^q]{\beta} = \alpha_s^{x_s} \Gamma^{\ell^{\mu-q}}, \quad x_s \not\equiv 0 \bmod. \ell$$

wenn $\sqrt[\ell^q]{\beta}$ die höchste in K mögliche Wurzel von β ist, also

$$\beta = \alpha_s^{x_s \ell^q} \Gamma^{\ell^\mu}$$

Wir betrachten nun $k(\Gamma) = k\left(\sqrt[\ell^\mu]{\beta \alpha_s^{-x_s \ell^q}}\right)$. Sei zunächst $q > 0$. Dann ist III, 76

*) Es ist ja $K(\sqrt[\ell^\mu]{\beta})$ dann $= K\left(\sqrt[\ell^{\mu-q}]{\sqrt[\ell^q]{\beta}}\right)$ wo $\sqrt[\ell^q]{\beta}$ keine ℓ–te Potenz mehr in K ist. Und da die ℓ^q–ten E. W. $\ell^{\mu-q}$–te Potenzen in K sind, ist die Normierung einerlei.

$\beta\alpha^{-x_s\ell^q}$ keine ℓ–te Potenz in k, da β keine ist. Dann folgt also nach Annahme für $s-1$:

$$\beta\alpha_s^{-x_s\ell^q} = \alpha_1^{x_1}\cdots\alpha_{s-1}^{x_{s-1}}\gamma^{\ell^\mu},$$

weil Γ in $K = k\left(\sqrt[\ell^{\nu_1}]{\alpha_1},\ldots,\sqrt[\ell^{\nu_{s-1}}]{\alpha_{s-1}}\right)$ liegt, also

$$\beta = \alpha_1^{x_1}\ldots\alpha_{s-1}^{x_{s-1}}\alpha_s^{x_s\ell^q}\gamma^{\ell^\mu},$$

und das ist eine Relation, wie behauptet. Wenn $q=0$ ist, also $\sqrt[\ell^\mu]{\beta\alpha^{-x_s}} = \Gamma$ in K liegt, so sei die ℓ^r–te Wurzel die höchste aus $\beta\alpha^{-x_s}$ in k ausziehbare $(0 \leqq r \leqq \mu)$. Für $r=\mu$ ist $\beta = \alpha^{x_s}\gamma^{\ell^\mu}$. Für $0 \leqq r < \mu$ ist

$$\Gamma = \sqrt[\ell^{\mu-r}]{\sqrt[\ell^r]{\beta\alpha^{-x_s}}} \quad \text{in } K$$

wo $\sqrt[\ell^r]{\beta\alpha^{-x_s}}$ keine ℓ–te Potenz in k ist, also nach Annahme:

$$\begin{aligned}\sqrt[\ell^r]{\beta\alpha^{-x_s}} &= \alpha_1^{x_1}\ldots\alpha_{s-1}^{x_{s-1}}\gamma^{\ell^{\mu-r}}\\ \beta\alpha^{-x_s} &= \alpha_1^{x_1\ell^r}\ldots\alpha_{s-1}^{x_{s-1}\ell^\mu}\gamma^{\ell^r}\end{aligned}$$

wie behauptet.

Daß in den gefundenen Relationen nicht alle Exponenten der $\alpha_1,\ldots,\alpha_s$ durch ℓ teilbar sein können, folgt aus dem Beweise, ist aber auch nach Annahme klar, daß β keine ℓ–te Potenz in k ist.

Satz 4. *Es enthalte k die ℓ^ν–ten und ℓ^μ–ten Einheitswurzeln, $(\nu,\mu \geqq 1)$, und es seien $\alpha_1,\ldots,\alpha_s$ beliebige Zahlen aus k, β eine solche Zahl die keine ℓ–te Potenz in k ist.*
Wenn dann

$$k\left(\sqrt[\ell^\mu]{\beta}\right) \prec k\left(\sqrt[\ell^\nu]{\alpha_1},\ldots,\sqrt[\ell^\nu]{\alpha_s}\right) = K$$

ist, so besteht eine Relation

$$\beta^{\ell^{\nu-1}} = \alpha_1^{x_1}\ldots\alpha_s^{x_s}\gamma^{\ell^\nu}$$

(wo über die $x_1,\ldots,x_s$ nichts Näheres ausgesagt wird).

III, 77

Beweis: Wir betrachten die Gruppe aller Potenzprodukte

$$\alpha_1^{x_1}\ldots\alpha_s^{x_s}\gamma^{\ell^\nu}; \quad (\gamma \text{ in } k)$$

mit mod. ℓ^ν genommenen Exponenten. Diese Abelsche Gruppe hat eine Untergruppe derjenigen Elemente, die ℓ^ν–te Potenzen in k sind. Es sei $\begin{pmatrix} x_{11} \dots x_{1s} \\ x_{r1} \dots x_{rs} \end{pmatrix}$ die Matrix der Exponenten einer Basis der zugehörigen Faktorgruppe, und $\beta_1, \dots, \beta_r$ die entsprechenden Potenzprodukte, die also Repräsentanten der Elemente der Faktorgruppe sind:

$$\beta_i = \prod_{k=1}^{s} \alpha_k^{x_{ik}} \gamma_i^{\ell^\nu}$$

Die β_i haben bestimmte Ordnungen in der Faktorgruppe, nämlich die frühesten Exponenten ℓ^{ϱ_i}, sodaß $\beta_i^{\ell^{\varrho_i}}$ ℓ^ν–te Potenz in k ist, und es ist $0 < \varrho_i \leqq \nu$. Wir denken uns diese Basiselemente nach fallenden Ordnungen geordnet:

$\beta_1, \dots, \beta_{r_1}$	Ordnung	ℓ^ν
$\beta_{r_1+1}, \dots, \beta_{r_1+r_2}$	"	$\ell^{\nu-1}$
....		
$\beta_{r_1+\dots+r_{\nu-1}+1}, \dots, \beta_{r_1+\dots+r_\nu}$	"	ℓ

(Im Falle der Unabhängigkeit von $\alpha_1, \dots, \alpha_s$ wie in Satz 3 können $\alpha_1, \dots, \alpha_s$ selbst als Basis genommen werden).

Sei β_i ein solches Basiselement der Ordnung ℓ^ϱ; $(0 < \varrho \leqq \nu)$. Dann ist also

$$\beta_i^{\ell^\varrho} = \gamma_i^{\ell^\nu}$$

d. h.

$$\beta_i = \gamma_i^{\ell^{\nu-\varrho}},$$

weil die ℓ^ϱ–ten E. W. $\ell^{\nu-\varrho}$–te Potenzen der ℓ^ν–ten E. W. sind. Daher können aus obigen Komplexen ja die ℓ^0–ten, ℓ^1–ten, ... $\ell^{\nu-1}$–ten Wurzeln ausgezogen werden. Es seien in der entsprechenden Reihenfolge $\alpha'_1, \dots, \alpha'_r$ die irgendwie normierten derartigen Wurzeln aus $\beta_1, \dots, \beta_r$. (Auf die Normierung kommt es, wie man sich leicht überlegt, nicht an, da daraus nur Übergang zu konjugierten, identischen Körpern entsteht). Nunmehr zeigen wir, daß K mit dem Körper: III, 78

$$K' = k\left(\sqrt[\ell^\nu]{\alpha'_1}, \dots, \sqrt[\ell^{\nu-1}]{\alpha'_{r_1+1}}, \dots \sqrt[\ell]{\alpha'_{r_1+\dots+r_{\nu-1}+1}}, \dots\right)$$

identisch ist. In der Tat ist nach Konstruktion K' bei gleichzeitiger Normierung

$$= k\left(\sqrt[\ell^\nu]{\beta_1}, \dots, \sqrt[\ell^\nu]{\beta_r}\right)$$

also in K enthalten, da die $\beta_1,\ldots,\beta_r$ bis auf ℓ^ν–te Potenzen Potenzprodukte der $\alpha_1,\ldots,\alpha_s$ sind. Andererseits aber haben $\alpha_1,\ldots,\alpha_s$ als Elemente unserer ursprünglichen Gruppe Darstellung durch die $\beta_1,\ldots,\beta_s$ als Basis der Faktorgruppe bis auf ℓ^ν–te Potenzfaktoren, sodaß K in K' enthalten ist.

Nun sind $\alpha'_1,\ldots,\alpha'_r$ in Bezug auf ℓ–te Potenzen unabhängig. Aus

$$\alpha'^{x_1}_1\cdots\alpha'^{x_r}_r=\gamma^\ell$$

folgt nämlich durch Potenzierung mit $\ell^{\nu-1}$:

$$\beta_1^{x_1\ell^{\nu-1}}\cdots\beta_{r_1+1}^{x_{r_1+1}\ell^{\nu-2}}\cdots\cdots\beta_{r_1+\cdots+r_{\nu-1}+1}^{x_{r_1+\cdots+r_{\nu-1}+1}}\cdots=\gamma^{\ell^\nu},$$

also da die $\beta_1,\ldots,\beta_r$ eine Basis unserer Faktorgruppe sind, daß jeder einzelne Faktor links ℓ^ν–te Potenz in k ist. Für ein β_i der Ordnung ℓ^ϱ folgt also eine Gleichung

$$\beta_i^{x\ell^{\varrho-1}}=\gamma_i^{\ell^\nu},$$

d. h. $x\equiv 0$ mod. ℓ. Somit müssen $x_1,\ldots,x_r\equiv 0$ mod. ℓ sein. Da nun $k\left(\sqrt[\ell^\mu]{\beta}\right)$ nach Voraussetzung in K, also in K' enthalten sein sollte, folgt nach Satz 3:

$$\beta=\alpha'^{x'_1}_1\cdots\alpha'^{x'_r}_r\gamma^{\ell^\mu},$$

d. h.

$$\beta^{\ell^{\nu-1}}=\beta_1^{x'_1\ell^{\nu-1}}\cdots\beta_{r_1+1}^{x'_{r_1+1}\ell^{\nu-2}}\cdots\beta_{r_1+\cdots+r_{\nu-1}+1}^{x'_{r_1+\cdots+r_{\nu-1}+1}}\cdots\gamma^{\ell^{\nu+\mu-1}}.$$

III, 79 Ersetzt man hierin die $\beta_1,\ldots,\beta_r$ durch die Potenzprodukte in $\alpha_1,\ldots,\alpha_s$, so folgt eine Relation

$$\beta^{\ell^{\nu-1}}=\alpha_1^{x_1}\ldots\alpha_s^{x_s}\gamma^{\ell^\nu},$$

wie behauptet.

Anmerkung 1: Wenn Potenzprodukte β_i der Ordnung ℓ^ϱ existieren, so ist das gleichbedeutend damit, daß sich aus gewissen Potenzprodukten der $\alpha_1,\ldots,\alpha_s$ die $\ell^{\nu-\varrho}$–te Wurzel ausziehen läßt, ohne daß alle Exponenten durch ℓ teilbar sind (sonst wäre β_i kein Basiselement). Setzt man nun voraus, daß sich aus keinem Potenzprodukt von $\alpha_1,\ldots,\alpha_s$ eine höhere als die ℓ^k–te Wurzel ausziehen läßt, wenn nicht alle Exponenten durch ℓ teilbar sind, so gibt es nur Basiselemente β_i der Ordnungen ℓ^ν, $\ell^{\nu-1},\ldots,\ell^{\nu-k}$, aber keine solchen von niedrigerer Ordnung. Dann folgt wie eben eine Relation

$$\beta^{\ell^k}=\beta_1^{x'_1\ell^k}\cdots\beta_{r_1+\cdots+r_{k+1}}^{x'_{r_1+\cdots+r_{k+1}}}\cdot\gamma^{\ell^{k+\mu}}$$

und durch Übergang zu den $\alpha_1, \ldots, \alpha_s$:

$$\beta^{\ell^k} = \alpha_1^{x_1} \ldots \alpha_s^{x_s} \gamma^{\ell^m}, \quad \text{wo } m = \mathrm{Min}(k+\mu, \nu)$$

Zusatz. *Ist in Satz 4 aus keinem Potenzprodukt von $\alpha_1, \ldots, \alpha_s$ eine höhere als die ℓ^k–te Wurzel ausziehbar, wenn nicht alle Exponenten durch ℓ teilbar sind, d. h. folgt aus*

$$\alpha_1^{x_1} \ldots \alpha_s^{x_s} = \gamma^{\ell^{k+1}},$$

daß $x_1, \ldots, x_s \equiv 0 \bmod. \ell$ sind, oder auch sind $\alpha_1, \ldots, \alpha_s$ in Bezug auf die ℓ^{k+1}–ten Potenzen unabhängig $(0 \leqq k \leqq \nu - 1)$, so besteht im Sinne von Satz 4 eine Relation

$$\beta^{\ell^k} = \alpha_1^{x_1} \ldots \alpha_s^{x_s} \gamma^{\ell^m} \quad \text{mit } \mathrm{Min}(k+\mu, \nu) = m$$

Anmerkung 2. Beim Beweis blieb der Fall unberücksichtigt, daß die betr. Faktorgruppe die Einheit ist. Dann sind alle $\alpha_1^{x_1} \ldots \alpha_s^{x_s}$ ℓ^ν–te Potenzen und $K = k$. Der Satz besagt dann, daß $\beta^{\ell^{\nu-1}} = \gamma^{\ell^\nu}$, also β eine ℓ–te Potenz in k ist. Aus dem Beweise folgt aber sofort, was auch an sich klar, daß β eine ℓ^μ–te Potenz in k sein muß. Im übrigen widerspricht aber dieser Fall der Voraussetzung, daß β keine ℓ–te Potenz in k sein soll, und somit ist obiger Beweis richtig verfahren, wenn er voraussetzte, daß die Faktorgruppe nicht die Einheit ist. III, 80

Satz 5. *Sind $\alpha_1, \ldots, \alpha_s$ in Bezug auf die Gruppe der ℓ–ten Potenzen in k unabhängig, enthält k die ℓ^ν–ten Einheitswurzeln $(\nu \geqq 1)$ und ist $1 \leqq \nu_1, \ldots, \nu_s \leqq \nu$, so ist*

$$K = k\,(\sqrt[\ell^{\nu_1}]{\alpha_1}, \ldots, \sqrt[\ell^{\nu_s}]{\alpha_s})$$

relativ–Abelsch über k vom Grade $\ell^{\nu_1+\cdots+\nu_s}$ und einer Gruppe vom Typus $(\ell^{\nu_1}, \ldots, \ell^{\nu_s})$.

Beweis: Es ist nur zu zeigen, daß der Grad $\ell^{\nu_1+\cdots+\nu_s}$ ist. Dann folgt das andere aus der Galoisschen Theorie für die Komposition zyklischer Körper. Nun ist nach der Galoisschen Theorie das Kompositum zweier teilerfremder Relativkörper, deren einer Galoissch ist, vom Produktgrade (Satz über akzessorische Irrationalitäten). Sei nun

$$K_i = k\,(\sqrt[\ell^{\nu_1}]{\alpha_1}, \ldots, \sqrt[\ell^{\nu_i}]{\alpha_i}), \quad \text{also} \quad K_s = K,$$

so ist

$$K_{i+1} = \left(K_i, k\left(\sqrt[\ell^{\nu_{i+1}}]{\alpha_{i+1}}\right)\right)$$

Da α_{i+1} keine ℓ–te Potenz in k ist, hat $k\left(\sqrt[\ell^{\nu_{i+1}}]{\alpha_{i+1}}\right)$ als einzige Teilkörper über k die Körper $k\left(\sqrt[\ell^{\varrho}]{\alpha_{i+1}}\right)$; $1 \leqq \varrho \leqq \nu_{i+1}$. Wäre nun der kleinster $k\left(\sqrt[\ell]{\alpha_{i+1}}\right)$ auch in K_i über k enthalten, so wäre nach Satz 3

$$\alpha_{i+1} = \alpha_1^{x_1} \cdots \alpha_i^{x_i} \gamma^{\ell},$$

entgegen der Voraussetzung. Daraus folgt alles mittels Satz 1.

3.13 Konstruktion von zyklischen Körpern gewisser Eigenschaften. (21.12.1924)

Hasse uses class field theory to prove the following result: if a number field k contains the ℓ-th roots of unity (or $i = \sqrt{-1}$ if $\ell = 2$), then there exist infinitely many cyclic extensions $K|k$ with degree ℓ^ν whose relative discriminant is divisible by a only one prime ideal, and this of degree 1 and coprime to ℓ.

III, 81

21. XII. 1924.

Es enthalte k die ℓ^μ–ten E. W. als höchste dieser Art ($\mu \geqq 1$, und $\geqq 2$ für $\ell = 2$), und es sei K der über k dann relativzyklische Körper ℓ^ν–ten Grades, der durch die Adjunktion der primitiven $\ell^{\nu+\mu}$–ten E. W. ($\nu \geqq 1$) erzeugt wird. Es sei ferner für den Körper k das System:

$$\zeta, \xi;\ \varepsilon_1, \dots, \varepsilon_r;\ \varrho_1, \dots, \varrho_e$$

das bekannte Basissystem von Einheitswurzeln ζ (Ordnung ℓ^μ), ξ (Ordnung prim zu ℓ), Grundeinheiten $\varepsilon_1, \dots, \varepsilon_r$ und unabhängigen ℓ–ten Idealpotenzen $\varrho_1, \dots, \varrho_e$, das auch zur Konstruktion der e singulären Primärzahlen (nach ℓ) benutzt wird, (indem eben die Untergruppe der ℓ–ten Potenzreste nach dem Modul $\mathfrak{l}_0^\ell$ des Kreiskörpers der ℓ–ten Einheitswurzeln den Rang e hat). Dann betrachten wir den Körper

$$\mathsf{K} = K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \dots \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \dots \right).$$

Wäre

$$\varrho = \varepsilon_1^{x_1} \dots \varrho_1^{y_1} \dots = \mathsf{A}^\ell \quad \text{in } K,$$

so wäre entweder A in k und dann bekanntlich $x_1, \dots, y_1, \dots$ durch ℓ teilbar, oder aber $k\left(\sqrt[\ell]{\varrho}\right)$ mit dem einzigen zyklischen Unterkörper ℓ–ten Grades $k\left(\sqrt[\ell]{\zeta}\right)$ von K über k identisch, also

$$\varrho = \zeta^x \gamma^\ell\,; \quad x \not\equiv 0 \text{ mod. } \ell.$$

Daher muß unter allen Umständen $x_1, \dots, y_1, \dots$ durch ℓ teilbar sein. K erfüllt also die Voraussetzungen von Satz 3 und 5 der vorigen Note]. Er ist also relativ–Abelsch vom Grade $\ell^{(r+e)(\nu+\mu)}$ über K, d. h. Klassenkörper nach einer Klassengruppe H in K von diesem Index nach einem Modul $\mathfrak{C}$, der nur Primteiler von ℓ enthält.

III, 82

Satz 1. *In H gibt es Ideale $\mathfrak{A}$ mit*

$$N(\mathfrak{A}) \not\equiv 1 \mod \ell^{\nu+\mu+1}$$

Beweis: Wäre stets $N(\mathfrak{A}) \equiv 1 \mod \ell^{\nu+\mu+1}$ für $\mathfrak{A}$ aus H, so wäre H in derjenigen Klassengruppe enthalten, nach der der Körper der $\ell^{\nu+\mu+1}$–ten Einheitswurzeln $K\left(\sqrt[\ell]{\mathsf{Z}}\right)$ Klassenkörper nach K ist. Dann wäre aber letzterer Unterkörper von K und somit nach Satz 3

$$\mathsf{Z} = \varepsilon_1^{x_1} \dots \varrho_1^{y_1} \dots \mathsf{A}^\ell\,; \quad \mathsf{A} \text{ in } K,$$

wo nicht alle $x_1, \dots, y_1, \dots \equiv 0$ mod. ℓ sind, sodaß also

$$\varrho = \varepsilon_1^{x_1} \dots \varrho_1^{y_1} \dots$$

nicht ℓ–te Potenz einer Zahl in k ist. Dann wäre aber

$$K\left(\sqrt[\ell]{\mathsf{Z}}\right) = K\left(\sqrt[\ell]{\varrho}\right) = \left(K, k(\sqrt[\ell]{\varrho})\right),$$

d. h. der zu k relativzyklische Körper $K\left(\sqrt[\ell]{\mathsf{Z}}\right)$ aus zwei zu K relativ–zyklischen Körpern der Grade ℓ^ν und ℓ, die teilerfremd sind, komponiert, was unmöglich.

Nach Satz 1 und Takagi gilt:

Satz 2. *Es gibt unendlich viele Primideale* 1. *Grades $\mathfrak{Q}$ in K, sodaß $\mathfrak{Q}$ in H und*

$$N(\mathfrak{Q}) = q \equiv 1 \mod \ell^{\nu+\mu}, \quad \text{aber } \not\equiv 1 \mod \ell^{\nu+\mu+1}.$$

Satz 3. *Die Restklassen* mod $\mathfrak{q}$ *liefern eine Gruppe von Idealklassen* mod $\mathfrak{q}$*, die einen direkten Faktor der Ordnung ℓ^ν enthält, und sonst nur Klassen mit zu ℓ primem Exponenten.*

Beweis: Die Ordnung der durch Hauptideale, also die $q-1$ primen Restklassen mod $\mathfrak{q}$ gelieferten Gruppe von Idealklassen mod $\mathfrak{q}$ hat die Ordnung $\frac{q-1}{(E:E_0)}$, wo $(E : E_0)$ den Index der Gruppe E_0 aller Einheiten $\equiv 1 \mod q$ zu der Gruppe E aller Einheiten von k bedeutet. Nun haben $\xi, \varepsilon_1, \dots, \varepsilon_r$ zu ℓ prime Exponenten mod $\mathfrak{q}$, weil sie $\ell^{\nu+\mu}$–te Potenzreste mod $\mathfrak{q}$ sind, $q-1$ *genau* durch $\ell^{\nu+\mu}$ teilbar ist, und die Restklassengruppe zyklisch ist. ζ hat genau den Exponenten

III, 83

ℓ^μ, da $\mathfrak{q}$ nur Teiler von $\zeta^x - 1$ sein kann, wenn $\zeta^x - 1 = 0$ ist, (q prim zu ℓ). Daher hat die Faktorgruppe von E_0 in E außer der durch ζ bestimmten zyklischen Untergruppe ℓ^μ–ter Ordnung nur Elemente mit zu ℓ primer Ordnung, d. h. ihre Ordnung ist genau durch ℓ^μ teilbar, d. h. $\frac{q-1}{(E:E_0)}$ genau durch ℓ^ν teilbar. Die Idealgruppe der Hauptideale mod $\mathfrak{q}$ hat daher einen direkten Faktor der Ordnung ℓ^ν (zyklisch), dessen komplementärer Faktor zu ℓ prime Ordnung hat, w. z. b. w.

Nun sei (γ) ein Hauptideal aus der Basisklasse der Ordnung ℓ^ν, ferner $\mathfrak{r}_1, \ldots, \mathfrak{r}_e$ ein System von Idealen aus den absoluten Basisklassen mit Exponenten ℓ^{ν_i}.

III, 84

Ferner sei (δ) ein Basisideal für die Hauptidealklassen mod $\mathfrak{q}$, mit zu ℓ primem Exponenten m, und $\mathfrak{t}_1, \ldots, \mathfrak{t}_g$ ein System von Idealen aus den absoluten Basisklassen mit zu ℓ primem Exponenten. Dann besteht für jedes Ideal $\mathfrak{a}$ aus k, das zu $\mathfrak{q}$ prim ist (auch alles übrige prim zu $\mathfrak{q}$, d. h. $\mathfrak{q}$ so gewählt), eine eindeutige Darstellung

$$\mathfrak{a} = (\gamma)^x (\delta)^y \mathfrak{r}_1^{x_1} \ldots \mathfrak{r}_\ell^{x_\ell} \mathfrak{t}_1^{y_1} \ldots \mathfrak{t}_g^{y_g} (\alpha),$$

wo $\alpha = 1 \mod \mathfrak{q}$ und die Exponenten nach den betr. Moduln reduziert sind. Die $\mathfrak{t}_1, \ldots, \mathfrak{t}_g$ mit den (absoluten) zu ℓ primen Exponenten $m_1, \ldots, m_g$ seien noch durch passende, zu $\mathfrak{q}$ prime Hauptidealfaktoren so normiert, daß ihre Idealklassen mod $\mathfrak{q}$ zu ℓ prime Exponenten haben. Das geht immer. Denn es sei

$$\mathfrak{t}_i^{m_i} = (\tau_i).$$

Ist nun

$$(\tau_i) = (\gamma)^{c_i} (\delta)^{d_i} (\alpha_i)\,; \quad \alpha_i \equiv 1 \mod \mathfrak{q},$$

so hat man nur $\mathfrak{t}_i(\beta_i)$ mit einem solchen (β_i) für $\mathfrak{t}_i$ zu setzen, daß

$$(\beta_i^{m_i})(\gamma^{c_i}) = (\delta)^{d_i'} (\alpha_i')\,; \quad \alpha_i' \equiv 1 \mod \mathfrak{q}$$

wird. Setzt man nun, wenn $m_i m_i' \equiv 1 \mod \ell^\nu$ ist:

$$(\beta_i) = (\gamma)^{-c_i m_i'},$$

so wird

III, 85

$$(\beta_i^{m_i})(\gamma^{c_i}) = (\gamma)^{-c_i m_i m_i' + c_i} = (\gamma)^{c\ell^\nu}.$$

Das letztere ist aber sogar die Hauptklasse mod $\mathfrak{q}$, weil (γ) die Ordnung ℓ^ν hat.

Sind die $\mathfrak{t}_1, \ldots, \mathfrak{t}_g$ so normiert, so ist ersichtlich durch

$$(\delta)^y \mathfrak{r}_1^{x_1} \ldots \mathfrak{r}_e^{x_e} \mathfrak{t}_1^{y_1} \ldots \mathfrak{t}_g^{y_g} (\alpha)\,; \quad \alpha \equiv 1 \mod \mathfrak{q}$$

eine Gruppe $G \mod \mathfrak{q}$ definiert. Denn die Produktbildung führt nach Wahl der $\mathfrak{t}_1, \ldots, \mathfrak{t}_g$ und da $(\varrho_1) = \mathfrak{r}_1^{\ell^{\nu_1}}, \ldots$ sämtlich $\ell^{\nu+\mu}$–te Potenzreste mod $\mathfrak{q}$ sind, also zu ℓ prime Exponenten mod $\mathfrak{q}$ haben, nicht aus diesem System heraus.

Daher ist die Gruppe $(\gamma)^x$ ein direkter Faktor der Gruppe aller Idealklassen mod $\mathfrak{q}$*, und ihr Komplement die eben bestimmte Gruppe G vom Index ℓ^ν.*

G ist ersichtlich nicht mod. 1 erklärbar. Also hat der zugehörige Klassenkörper den Primfaktor $\mathfrak{q}$ in der Relativdiskriminante, und zwar als einzigen Primfaktor, und ist zyklisch von der Ordnung ℓ^ν über k. Also gilt:

Satz 4. *Enthält k die ℓ–ten und für $\ell = 2$ die 2^2–ten Einheitswurzeln, so gibt es unendlich viele verschiedene relativ–zyklische Körper ℓ^ν–ten Grades über k, in deren Relativdiskriminante je nur ein einziges Primideal* 1. *Grades $\mathfrak{q}$ von k aufgeht, das nicht in ℓ aufgeht.*

Um die Schwierigkeit der Normierung der $\mathfrak{t}_1, \ldots, \mathfrak{t}_g$ zu vermeiden, darf man sie von vorneherein durch ihre $\ell^{\nu+\mu}$-ten Potenzen ersetzt denken, sodaß dann die m_i–ten Potenzen von selbst $\ell^{\nu+\mu}$–te Potenzen von Hauptidealen werden. Dies sei für das folgende als geschehen vorausgesetzt, sodaß jetzt die $\mathfrak{t}_i$ *fest* gewählt sind, und $\mathfrak{q}$ prim zu ihnen zu bestimmen ist. Dann ist *ohne* Normierung

III, 86

$$\mathfrak{r}_1^{x_1} \ldots \mathfrak{r}_e^{x_e} \mathfrak{t}_1^{y_1} \ldots \mathfrak{t}_e^{y_e} (\delta)^y (\alpha)\,; \quad \alpha \equiv 1 \mod \mathfrak{q}$$

eine Gruppe.

Soll nun ein vorgegebenes, zu ℓ primes Primideal $\mathfrak{p}$ von k im zu konstruierenden zyklischen Körper ℓ^ν–ten Grades in verschiedene Primideale ℓ^κ–ten Grades $(0 \leqq \kappa \leqq \nu)$ zerfallen, und ist

$$\mathfrak{p} = \mathfrak{r}_1^{x_1} \ldots \mathfrak{r}_e^{x_e} \mathfrak{t}_1^{y_1} \ldots \mathfrak{t}_g^{y_g} \ (\pi),$$

wobei nun alles auch zu $\mathfrak{p}$ prim angenommen werde, so muß $\mathfrak{p}^{\ell^\kappa}$ in G, aber $\mathfrak{p}^{\ell^{\kappa-1}}$ (falls $\kappa > 0$) noch nicht in G liegen. Das bedeutet aber nach dem a. d. S. oben bemerkten, daß $(\pi)^{\ell^\kappa}$ in $(\delta)^y(\alpha)$, aber $(\pi)^{\ell^{\kappa-1}}$ noch nicht sein muß. Nun besteht $(\delta)^y(\alpha)$ aus allen Hauptidealklassen mod $\mathfrak{q}$, die zu ℓ prime Exponenten haben. Es genügt, wenn wir

$$\pi^{\ell^\kappa} \equiv \xi^{\ell^{\nu+\mu}} \mod \mathfrak{q}$$

fordern. Andererseits muß $(\pi)^{\ell^{\kappa-1}}$ in einer Klasse mit durch ℓ teilbarem Exponenten liegen. Da nun die sämtlichen Klassen mit zu ℓ primem Exponenten aus

den $\ell^{\nu+\mu}$–ten Potenzresten unter Hinzunahme der Einheiten enthalten, genügt es zu fordern

$$\pi^{\ell^{\kappa-1}} \not\equiv \zeta^x \xi^{\ell^{\nu+\mu}} \mod \mathfrak{q}.$$

Wir haben demnach, wenn wir in K zu $\mathfrak{Q}$ übergehen, zu fordern:

$$\begin{aligned} &\pi \equiv \Xi^{\ell^{\nu+\mu-\kappa}} \mod \mathfrak{Q}, \\ &\pi \mathsf{Z}^{x\ell^{\nu-\kappa+1}} \not\equiv \Xi^{\ell^{\nu+\mu-\kappa+1}} \mod \mathfrak{Q} \quad \text{für} \quad x = 0, 1, \ldots \ell^{\mu+\kappa-1} - 1, \end{aligned}$$

wo $\mathsf{Z}^{\ell^{\nu-\kappa+1}}$ eine primitive $\ell^{\mu+\kappa-1}$–te Einheitswurzel ist. Das bedeutet, daß $\mathfrak{Q}$ in der Klassengruppe P von III, 87

$$K\left(\sqrt[\ell^{\nu+\mu-\kappa}]{\pi}\right),$$

aber nicht in den $\ell^{\mu+\kappa-1}$ Klassengruppen $\mathsf{P}_1, \mathsf{P}_2, \ldots$ der Körper

$$K\left(\sqrt[\ell^{\nu+\mu-\kappa+1}]{\pi \mathsf{Z}^{x\ell^{\nu-\kappa+1}}}\right)$$

vorkommt, und es ist die Frage, ob dies mit den bisherigen Bestimmungsforderungen vereinbar ist.

Es sei nun

C	die	Idealgruppe	$N(\mathfrak{A}) \equiv 1 \mod \ell^{\nu+\mu+1}$	von	K
H	"	"	zu $K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \ldots \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \ldots\right)$	"	"
P	"	"	zu $K\left(\sqrt[\ell^{\nu+\mu-\kappa}]{\pi}\right)$	"	"
P_x	"	"	zu $K\left(\sqrt[\ell^{\nu+\mu-\kappa+1}]{\pi \mathsf{Z}^{x\ell^{\nu-\kappa+1}}}\right)$	"	"

Wir bezeichnen nun mit $\overline{K}$ den Körper der $\ell^{\nu+2\mu}$–ten E. W. über k und K, relativ–zyklisch über K vom Grade ℓ^μ, ferner setzen wir

$$\begin{aligned} \mathsf{K} &= K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \ldots \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \ldots \sqrt[\ell^{\nu+\mu-\kappa}]{\pi}\right) \\ \mathsf{K}_x &= K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \ldots \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \ldots \sqrt[\ell^{\nu+\mu-\kappa+1}]{\pi \mathsf{Z}^{x\ell^{\nu-\kappa+1}}}\right) \end{aligned}$$

und mit $\overline{\mathsf{K}}$ und $\overline{\mathsf{K}}_0$ die entsprechenden Körper über $\overline{K}$, wobei zu bemerken ist, daß die K_x sich wegen $\sqrt[\ell^{\nu+\mu-\kappa+1}]{\mathsf{Z}^{x\ell^{\nu-\kappa+1}}} = \sqrt[\ell^\mu]{\mathsf{Z}}^{\,x}$ relativ $\overline{K}$ nicht mehr unterscheiden, sodaß also $\overline{\mathsf{K}}_0$ zyklisch vom ℓ–ten Grade über $\overline{\mathsf{K}}$ ist. Ferner sind relativ zu K die Körper $\overline{K}$ und K bzw. K_x teilerfremd. Sonst wäre nämlich $\sqrt[\ell]{\mathsf{Z}}$ in K bzw. K_x enthalten, also wegen der leicht zu zeigenden Unabhängigkeit der Radikanden von K und K_x (π enthält keine ℓ–ten Idealpotenzen in K)

$$\mathsf{Z} = \varepsilon_1^{x_1} \cdots \varrho_1^{y_1} \cdots \left(\pi \mathsf{Z}^{x\ell^{\nu-\kappa+1}}\right)^z \mathsf{A}^\ell$$

III, 88 was ebenso als unmöglich erwiesen wird. Daher sind $\overline{\mathsf{K}}$, $\overline{\mathsf{K}}_0$ über K teilerfremd komponiert:

$$\left.\begin{array}{l}\overline{\mathsf{K}} = (\overline{K}, \mathsf{K}) \\ \overline{\mathsf{K}}_0 = (\overline{K}, \mathsf{K}_x) \quad \text{für alle } x\end{array}\right\} \text{relativ } K.$$

Weil $\overline{\mathsf{K}}_0$ größer als $\overline{\mathsf{K}}$ ist, gibt es in $\overline{K}$ Primideale, die in $\overline{\mathsf{K}}$ vollständig zerfallen, in $\overline{\mathsf{K}}_0$ nicht, und zwar unendlich viele vom 1. Grade. Deren Relativnormen haben dieselbe Eigenschaft bezüglich K und K bzw. der K_x, wie leicht einzusehen. Also sind sie in H, P, nicht in $P_1, P_2, \ldots$ enthalten, leider aber noch *naturgemäß* in C. Jedenfalls ergibt sich aber, daß die in H, P und nicht in $P_1, P_2, \ldots$ enthaltenen Ideale von K eine *nicht leere* Gesamtheit von Strahlklassen nach einem geeigneten Modul bilden. Es ist nun nur noch zu zeigen, daß darunter auch *nicht in* C befindliche Ideale vorkommen.

23. XII. 24. Mit denselben Hilfsmitteln wie im folgenden, stellt sich heraus, daß eine derartige Bestimmung unmöglich ist, indem *alle* Ideale, die in H, P, aber nicht in $P_1, P_2, \ldots$ sind, notwendig in C liegen. Der obige Ansatz von π erweist sich als zu speziell, das Beispiel $k = R(\sqrt{-3})$, $\mu = 1$, $\nu = 1$, $\kappa = 1$, $p = 5$, $q = 19$ zeigt vielmehr, daß die bei π^{ℓ^κ} auftretende ℓ^μ–te Einheitswurzel *nicht* vernachlässigt werden darf. Wir wählen sie jetzt im Gegenteil sogar *primitiv*, erhalten also folgende Forderungen:

$$\begin{array}{rcl}\pi^{\ell^\kappa} & \equiv & \mathsf{Z}^{-\ell^\nu}\Xi^{\ell^{\nu+\mu}} \mod \mathfrak{Q} \\ \pi^{\ell^{\kappa-1}} & \not\equiv & \mathsf{Z}^{-x\ell^\nu}\Xi^{\ell^{\nu+\mu}} \mod \mathfrak{Q}\end{array}$$

d. h.

$$\begin{array}{rcl}\pi & \equiv & \mathsf{Z}^{-\ell^{\nu-\kappa}}\Xi^{\ell^{\nu+\mu-\kappa}} \mod \mathfrak{Q} \\ \pi & \not\equiv & \mathsf{Z}^{-x\ell^{\nu-\kappa+1}}\Xi^{\ell^{\nu+\mu-\kappa+1}} \mod \mathfrak{Q}.\end{array}$$

III, 89 Wir bezeichnen nunmehr abweichend von vorhin die auftretenden Körper und Gruppen so:

$$\mathsf{K} = K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \ldots, \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \ldots, \sqrt[\ell^{\nu+\mu-\kappa}]{\pi\mathsf{Z}^{\ell^{\nu-\kappa}}}\right)$$

zugeordnete Gruppe H

$$\mathsf{K}_x = K\left(\sqrt[\ell^{\nu+\mu}]{\varepsilon_1}, \ldots, \sqrt[\ell^{\nu+\mu}]{\varrho_1}, \ldots, \sqrt[\ell^{\nu+\mu-\kappa}]{\pi\mathsf{Z}^{\ell^{\nu-\kappa}}}, \sqrt[\ell^{\nu+\mu-\kappa+1}]{\pi\mathsf{Z}^{x\ell^{\nu-\kappa+1}}}\right)$$

$$\shortparallel \qquad\qquad \shortparallel \qquad H_x$$

$$\overline{K} = K\left(\sqrt[\ell]{\mathsf{Z}}\right)$$

$$\shortparallel \qquad\qquad \shortparallel \qquad C$$

Es sind dann die H_x Untergruppen von H, und unsere Forderungen kommen darauf hinaus, daß $\mathfrak{Q}$ in H, aber nicht in den H_x und nicht in C liegen soll. Die Radikanden, die bei K auftreten sind von einander unabhängig, wie leicht zu zeigen. Aus demselben Grunde kann K nicht $\overline{K}$ enthalten. Daher ist der Durchschnitt (H, C) eine Untergruppe vom Index ℓ von H. Ferner ist K_x vom Relativgrad $\ell^{\mu+1}$ über K. Es ist nämlich

$$\mathsf{K}_x = \mathsf{K}\left(\sqrt[\ell^{\mu+1}]{\sqrt[\ell^{\nu-\kappa}]{\pi} \cdot \mathsf{Z}^{\ell x}}\right)$$

wobei $\sqrt[\ell^{\nu-\kappa}]{\pi} = \left(\sqrt[\ell^{\nu+\mu-\kappa}]{\pi \mathsf{Z}^{\ell^{\nu-\kappa}}}\right)^{\ell^{\mu}} \cdot \mathsf{Z}^{-1}$ in K liegt und natürlich auch $\mathsf{Z}^{\ell x}$. Wäre nun K_x von niedrigerem Grade, so wäre $\sqrt[\ell^{\nu-\kappa}]{\pi}\mathsf{Z}^{\ell x}$, also auch $\sqrt[\ell^{\nu-\kappa}]{\pi}$ selbst ℓ–te Potenz in K, d. h. auch noch $\sqrt[\ell^{\nu-\kappa+1}]{\pi}$ in K vorhanden.
Dann wäre aber auch

$$\frac{\sqrt[\ell^{\nu-\mu+1}]{\pi \mathsf{Z}^{\ell-\kappa}}}{\sqrt[\ell^{\nu-\kappa+1}]{\pi}} = \sqrt[\ell]{\mathsf{Z}}$$

in K enthalten, was wie eben gesagt, nicht der Fall ist. Daher haben alle H_x den Index $\ell^{\mu+1}$ unter H. Wir denken uns nun H nach einem so hohen Modul erklärt, daß auch alle H_x und C danach erklärbar sind. Dann zählen wir ab, der wievielte Teil aller Nebengruppen nach der Strahlhauptklasse von H durch die H_x und den Durchschnitt (H, C) geliefert wird. Im allerhöchsten Falle wird nun der Teil $\frac{\ell^{\mu}}{\ell^{\mu+1}}$ von H durch die H_x eingenommen, weil genau ℓ^{μ} verschiedene Körper K_x vorhanden sind, und jedes H_x genau einen Teil $\frac{1}{\ell^{\mu+1}}$ aller Nebengruppen ausmacht. Da die H_x ferner sämtlich eine Untergruppe, nämlich den Durchschnitt $(H, H_1, H_2, \dots H_{\ell^{\mu}})$ gemeinsam haben, ist der Bruchteil $< \frac{\ell^{\mu}}{\ell^{\mu+1}} = \frac{1}{\ell}$. Der Bruchteil von (H, C) ist genau $\frac{1}{\ell}$, also der von beiden zusammen eingenommene $< \frac{2}{\ell} \leqq 1$, also < 1, womit gezeigt ist, daß es Nebengruppen nach dem obigen Modul für H gibt, die nicht in den H_x und nicht in C enthalten sind. Sonach gilt:

III, 90

Satz 5. *Enthält k die ℓ–ten (2^2–ten) Einheitswurzeln, so gibt es unendlich viele relativ–zyklische Körper ℓ^{ν}–ten Grades über k (ν beliebig $\geqq 1$), in deren Relativdiskriminante nur ein einziges zu ℓ primes Primideal 1. Grades $\mathfrak{q}$ aufgeht, und in denen ein vorgegebenes Ideal $\mathfrak{p}$ von k in Faktoren ℓ^{κ}–ten Grades zerfällt, wobei $0 \leqq \kappa \leqq \nu$ beliebig und $\mathfrak{p}$ prim zu ℓ.*

3.14 Ableitung der Partialbruchzerlegung von $\frac{\pi^2}{\sin^2 \pi z}$ nach Herglotz. (9.10.1925)

This deals with the "Herglotz trick", communicated to Hasse by Artin. See [Els98].

III, 91

9. X. 1925

(Nach brieflicher Mitteilung von E. Artin).

Satz. $\left(\frac{\pi}{\sin \pi z}\right)^2 = \sum_{\nu=-\infty}^{+\infty} \frac{1}{(z-\nu)^2}.$

Beweis: $\varphi(z) = \left(\frac{\pi}{\sin \pi z}\right)^2 - \sum_{\nu=-\infty}^{+\infty} \frac{1}{(z-\nu)^2}$. Diese Funktion $\varphi(z)$ hat folgende 3 Eigenschaften:

1.) $\varphi(z+1) = \varphi(z)$

2.) $\varphi(z)$ ist überall stetig.

denn für $z \neq \nu$ ist das trivial, für $z = \nu$ hat $\frac{\pi}{\sin \pi z}$ einen Pol 1. Ordnung mit dem Residuum 1, d. h. ist $\frac{\pi}{\sin \pi z} = \frac{1}{z-\nu} + \cdots$ $\left(\lim_{z \to \nu} \frac{\pi(z-\nu)}{\sin \pi z} = \frac{\pi}{\pi \cos \pi \nu} = 1\right)$.

3.) $\varphi(z) = \frac{1}{4}\left(\varphi\left(\frac{z}{2}\right) + \varphi\left(\frac{z+1}{2}\right)\right)$

Denn $$\varphi\left(\frac{z}{2}\right) = \left(\frac{\pi}{\sin \frac{\pi z}{2}}\right)^2 - \sum_{\nu=-\infty}^{+\infty} \frac{1}{\left(\frac{z}{2}-\nu\right)^2} = \frac{\pi^2}{\sin^2 \frac{\pi}{2} z} - 4 \sum_{\nu=-\infty}^{+\infty} \frac{1}{(z-2\nu)^2}$$

$$\varphi\left(\frac{z+1}{2}\right) = \left(\frac{\pi}{\sin \frac{\pi(z+1)}{2}}\right)^2 - \sum_{\nu=-\infty}^{+\infty} \frac{1}{\left(\frac{z+1}{2}-\nu\right)^2} =$$

$$= \frac{\pi^2}{\cos^2 \frac{\pi}{2} z} - 4 \sum_{\nu=-\infty}^{+\infty} \frac{1}{\big(z-(2\nu-1)\big)^2}$$

$$\varphi\left(\frac{z}{2}\right) + \varphi\left(\frac{z+1}{2}\right) = \frac{4\pi^2}{\sin^2 z} - 4 \sum_{\nu=-\infty}^{+\infty} \frac{1}{(z-\nu)^2} = 4\varphi(z).$$

Nach 1.) und 2.) ist $\varphi(z)$ im Reellen beschränkt: $|\varphi(z)| < C$.
Nach 3.) folgt dann für reelle z:

$$|\varphi(z)| < \frac{1}{4}(C + C) = \frac{C}{2}$$

Also $|\varphi(z)| <$ jedes $\frac{C}{2^n}$, also $|\varphi(z)| = 0$, d. h. $\varphi(z) = 0$.

Für komplexe z entweder funktionentheoretisch *direkt* oder durch Operieren mit Kreis, der so groß, daß mit z auch $\frac{z}{2}$ und $\frac{z+1}{2}$ darin, zweimalige Integration liefert das Produkt.

3.15 Ein Satz über die Körperdiskriminante. (9.10.1925)

Hasse gives Stickelberger's proof of his congruence for the discriminant. See [Lem00].

III, 92

9. X. 1925

(Stickelbergers Beweis, mitgeteilt durch Bessel–Hagen).
(siehe Ber. ü. d. intern. Math. Kongr. Zürich 1897).

Satz. *Ist d die Diskriminante eines algebraischen Zahlkörpers, p eine ungerade, nicht in d aufgehende Primzahl, n der Grad des Körpers und m die Anzahl der Primfaktoren von p in ihm, so gilt*

$$\left(\frac{d}{p}\right) = (-1)^{n-m}.$$

Ferner ist stets $\left(\frac{d}{4}\right) = 1$ (*d. h.* $d \equiv 0$ *oder* $1 \bmod. 4$) *und, falls* 2 *nicht in d aufgeht,* (*also* $d \equiv 1 \mod 4$) *ist,*

$$\left(\frac{d}{8}\right) = (-1)^{n-m},$$

wenn 2 *in m verschiedene Primfaktoren zerfällt.*

Beweis: Es sei K der zugeordnete Galoissche Körper, $\mathfrak{G}$ seine Galoissche Gruppe, die wir uns durch Permutationen der n konjugierten dargestellt denken. Geht die (gerade oder ungerade) Primzahl p nicht in d, also auch nicht in der Diskriminante von K auf, so ist bekanntlich jede der zu p gehörigen (konjugierten) Zerlegungsgruppen $\mathfrak{G}$ zyklisch. Es sei σ die erzeugende Substitution einer solchen Zerlegungsgruppe. Dann gilt nach einem Satz von Frobenius, der in der folgenden Note] hergeleitet ist, eine Zerlegung

$$\sigma = \zeta_1 \ldots \zeta_m$$

in m Zyklen $\zeta_1, \ldots, \zeta_m$ ohne gemeinsame Elemente.

a.) $\mathfrak{G}$ enthält nur gerade Permutationen. Da dann $\sqrt{d} = |\omega_i^{(k)}|$ bei allen Permutationen von $\mathfrak{G}$ invariant bleibt, ist $\sqrt{d}$ rational, d. h. d Quadratzahl, also

$\left(\frac{d}{p}\right) = 1$ bezw. $\left(\frac{d}{8}\right) = 1$. Andererseits ist $\operatorname{sgn}\zeta = \zeta^{f-1}$, wenn f der Grad von ζ ist. Da nun nach Annahme σ gerade ist, ist III, 93

$$1 = \operatorname{sgn}\sigma = (-1)^{f_1+f_2+\cdots+f_m-m} = (-1)^{n-m}.$$

b.) $\mathfrak{G}$ enthält auch ungerade Permutationen. Dann bilden die geraden Permutationen einen Normalteiler $\mathfrak{H}$ von $\mathfrak{G}$ vom Index 2. Zu $\mathfrak{H}$ gehört ein quadratischer Unterkörper L von K, der durch die genau bei $\mathfrak{H}$ invariante Größe $\sqrt{d}$ erzeugt wird. $\left(\frac{d}{p}\right)$ bezw. $\left(\frac{d}{8}\right)$ gibt an, ob p in L zerfällt, oder nicht. Wie unter a.) ist wieder $\operatorname{sgn}\sigma = (-1)^{n-m}$. Ist nun $\operatorname{sgn}\sigma = (-1)^{n-m} = 1$, so gehört σ zu $\mathfrak{H}$, also ist $\mathfrak{G}_2 \prec \mathfrak{H}$, d. h. der Zerlegungskörper $K_Z \succ L$. Also kann p in L nicht unzerlegt bleiben, d. h. es ist $\left(\frac{d}{p}\right)$ bzw. $\left(\frac{d}{8}\right) = 1$. Ist umgekehrt letzteres der Fall, so zerfällt p in L in verschiedene Primideale 1. Grades. Nach einem in der zweitfolgenden Note] hergeleiteten Satz über den Zerlegungskörper ist also $L \prec K_Z$, $\mathfrak{G}_Z \prec \mathfrak{H}$, also σ gerade, d. h. $(-1)^{n-m} = 1$.

Daß $d \equiv 1 \bmod. 4$ sein muß, folgt daraus, daß für $d \equiv 3 \mod 4$ sicher 2 in der Diskriminante von L, also von K aufginge, was nach Annahme nicht der Fall.

c.) Es bleibt noch zu zeigen, daß, wenn 2 in d aufgeht, sogar $d \equiv 0 \bmod. 4$ ist. Im Falle a.) ist das klar. Im Falle b.) (sowie überhaupt) kann $d = 2^1 d_0$ mit $(d_0, 2) = 1$ nur so zustande kommen, daß $2 = \mathfrak{p}_1^2 \mathfrak{p}_2 \cdots \mathfrak{p}_m$ mit $\mathfrak{p}_1$ vom Grade 1 ist. Da dann aber der Exponent $e_1 = 2$ von $\mathfrak{p}_1$ durch 2 teilbar ist, ist die Verzweigungsordnung $\bar{e}_1 > 2$, d. h. d durch mindestens 2^2 teilbar, (nämlich durch $2^{\bar{e}_1 - 1}$).

3.16 Ein Satz von Frobenius. (9.10.1925)

The prime decomposition of an unramified prime can be read off from the cycle decomposition of a generator of its decomposition group. This is a theorem of Frobenius, and Hasse extracts its proof from Artin's paper on zeta functions [Art23].

III, 94

9. X. 1925.

(Aus E. Artin, Ann. **89**, S. 147 ff).

Satz. *Ist k ein algebraischer Körper über k_0 K der zugehörige Galoissche Körper, $\mathfrak{G}$ die Galoissche Gruppe von K, $\mathfrak{p}_0$ ein nicht in der Relativdiskriminante von k (also auch von K) aufgehendes Primideal von k_0. Stellt man $\mathfrak{G}$ durch die Permutationen der zu k konjugierten dar, und zerfällt die Erzeugende σ einer der zu $\mathfrak{p}_0$ gehörigen (konjugierten) Zerlegungsgruppen (die ja zyklisch sind) in m Zyklen ohne gemeinsame Elemente der Grade $f_1, \ldots, f_m$, so besteht für $\mathfrak{p}_0$ in k eine Zerlegung*

$$\mathfrak{p}_0 = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_m\,; \quad (\mathfrak{p}_i \text{ vom Relativgrade } f_i).$$

Beweis: k gehöre zur Untergruppe $\mathfrak{g}$ von $\mathfrak{G}$. Wir wenden $\mathfrak{g}$ auf die Primfaktoren $\mathfrak{P}$ von $\mathfrak{p}_0$ in K an. Dadurch mögen diese in m Gruppen $\mathfrak{P}_{i1}, \ldots, \mathfrak{P}_{ir_i}$ $(i = 1, \ldots, m)$ zerfallen, derart, daß immer alle und nur die Primfaktoren einer solchen Gruppe durch $\mathfrak{g}$ auseinander entstehen. Dann sind die Ideale

$$\mathfrak{p}_i = \mathfrak{P}_{i1} \ldots \mathfrak{P}_{ir_i} \quad (i = 1, \ldots, m)$$

Primideale in k. Denn erstens gehören sie zu k, weil sie bei den Substitutionen der Galoisschen Gruppe $\mathfrak{g}$ von K nach k invariant sind (Ist $\mathfrak{p} = \mathfrak{P} \cdot \sigma_2 \mathfrak{P} \ldots \sigma_r \mathfrak{P}$ die Zerlegung eines Primideals $\mathfrak{p}$ eines Körpers k in einem Galoisschen Oberkörper K, und ist $\mathfrak{A}$ ein bei der Gruppe von K invariantes Ideal aus K, so enthält $\mathfrak{A}$ mit $\mathfrak{P}$ auch $\sigma_2 \mathfrak{P}, \ldots$ alle in derselben Potenz, d. h. enthält *genau* eine Potenz von $\mathfrak{p}$, d. h. ist Ideal in k), zweitens sind sie Primideale, weil kein Teiler von ihnen in k liegt. Wegen

$$\mathfrak{p}_0 = \prod_{i,k} \mathfrak{P}_{ik}$$

III, 95

ist auch

$$\mathfrak{p}_0 = \prod_{i=1}^{m} \mathfrak{p}_i.$$

Es sei f_i der Relativgrad von $\mathfrak{p}_i$ und $\tau_{ik}\mathfrak{P} = \mathfrak{P}_{ik}$. Dann werden die konjugierten Zerlegungsgruppen durch

$$\sigma_{ik} = \tau_{ik}^{-1}\sigma\tau_{ik}$$

erzeugt. Es seien $\mathfrak{G}_{ik}$ diese Zerlegungsgruppen, dann sind $\mathfrak{g}_{ik} = [\mathfrak{G}_{ik}, \mathfrak{g}]$ die relativ zu k. Sind f, f_i, $\overline{f}_i$ die Relativgrade der $\mathfrak{P}_{ik}$ zu k_0, $\mathfrak{p}_i$ zu k, $\mathfrak{P}_{ik}$ zu k, so gilt bekanntlich $f = f_i\overline{f}_i$. Da $\mathfrak{G}_{ik}$ zyklisch von der Ordnung f ist, und $\mathfrak{g}_{ik}$ zyklisch von der Ordnung $\overline{f}_i$, muß $\mathfrak{g}_{ik}$ durch $\sigma_{ik}^{f_i}$ erzeugt werden. Somit ist $\sigma_{ik}^{f_i}$ die niedrigste Potenz von σ_{ik}, die zu $\mathfrak{g}$ gehört, d. h. die die k zugeordnete Ziffer 1 festläßt. Die Ziffer 1 liegt also in σ_{ik} in einem Zyklus von f_i Elementen. Somit enthält auch die transformierte σ einen Zyklus von f_i Elementen.

Würden nun σ_{ik} und σ_{jh} auf diese Weise auf denselben f_i–gliedrigen Zyklus in σ führen, so müßte zunächst $f_i = f_j$ sein. Sei etwa

$$\sigma_{ik} = (1\ a_2\ \ldots\ a_{f_i})\ \ldots,\ \sigma_{jh} = (1\ b_2\ \ldots\ b_{f_i})\ \ldots$$
$$\tau_{ik} = \begin{pmatrix} c_1 & c_2 \ldots & c_{f_i} \ldots \\ 1 & a_2 \ldots & a_{f_i} \ldots \end{pmatrix}$$

also

$$\sigma = \tau_{ik}\sigma_{ik}\tau_{ik}^{-1} = (c_1\ c_2\ \ldots\ c_{f_i}) \cdots$$

Sollte nun aus σ_{jh} derselbe Zyklus in σ entstehen, so müßte τ_{jh} von der Form sein

$$\tau_{jh} = \begin{pmatrix} c_{\nu+1} & c_{\nu+2} \cdots & c_{\nu+f_i} \cdots \\ 1 & b_2 \ldots & b_{f_i} \ldots \end{pmatrix}$$

wo oben die Indizes mod f_i geschrieben sind. Dann wäre also $\tau_{ik}^{-1}\tau_{jh}\sigma_{jh}^{\nu}$ eine Permutation, bei der $0, a_2, \ldots, a_{f_i}$ zunächst durch τ_{ik}^{-1} in $c_1, \ldots, c_{f_i}$, diese durch τ_{jh} in $b_{1-\nu}, \ldots, b_{f_i-\nu}$ ($b_1 = 1$ gesetzt!), und diese durch σ_{jh}^{ν} in $b_1, \ldots, b_k$ d. h. $1, b_2, \ldots, b_r$ übergehen. Es bleibt also 1 bei $\tau_{ik}^{-1}\tau_{jh}\sigma_{jh}^{\nu}$ invariant, d. h. diese Permutation liegt in $\mathfrak{g}$. Dann folgte aber III, 96

$$\tau_{ik}^{-1}\tau_{jh}\sigma_{jh}^{\nu}\mathfrak{P}_{ik} = \tau_{jh}\sigma_{jh}^{\nu}\mathfrak{P} = \sigma_{jh}^{\nu}\mathfrak{P}_{jh} = \mathfrak{P}_{jh}$$

d. h. $\mathfrak{P}_{ik}$ und $\mathfrak{P}_{jh}$ hängen durch eine Permutation aus $\mathfrak{g}$ zusammen. Dann wäre aber $i = j$. Daher entsprechen den verschiedenen $\mathfrak{p}_i$ auch verschiedene Zyklen von f_i Elementen in σ. Da bekanntlich $\sum_{i=1}^{m} f_i = n$ der Relativgrad von k über k_0 und somit die Anzahl der Ziffern unserer Permutationen ist, sind damit alle Zyklen von σ erschöpft.

3.17 Ein Satz über den Zerlegungskörper. (9.10.1925)

A remark on the decomposition field which Hasse extracts from Hilbert's Zahlbericht.

III, 97

9. X. 25

Satz. *Es sei k ein algebraischer Körper, K ein relativ–Galoisscher Körper über k, $\mathfrak{p}$ ein Primideal aus k und $\overline{K}$ ein solcher Körper zwischen k und K, daß $\mathfrak{p}$ in $\overline{K}$ einen Primfaktor $\overline{\mathfrak{P}}$ vom Relativgrade 1 bekommt, der nicht in der Relativdifferente von $\overline{K}$ nach k aufgeht. Dann ist $\overline{K}$ Unterkörper der zu $\overline{\mathfrak{P}}$ gehörigen Zerlegungskörper von K nach k.*

Beweis: Nach Satz 76 des Zahlberichts ist zunächst $\overline{K}$ Unterkörper der zu $\overline{\mathfrak{P}}$ gehörigen Trägheitskörper K_T. Sei ferner K_Z ein zu $\overline{\mathfrak{P}}$ gehöriger Zerlegungskörper, $\mathfrak{P}_Z$ das entsprechende Primideal, sodaß $\left[\mathfrak{P}_Z, \overline{\mathfrak{P}}\right]$ ein von 1 verschiedenes Ideal des Kompositums $(K_Z, \overline{K})$ ist. Man zeigt leicht, daß jede für $\mathfrak{p}$ ganze Zahl aus diesem Kompositum mod $\left[\mathfrak{P}_Z, \overline{\mathfrak{P}}\right]$ einer Zahl aus k kongruent ist, weil dies für die für $\mathfrak{p}$ ganzen Zahlen aus K_Z mod $\mathfrak{P}_Z$ und aus $\overline{K}$ mod $\overline{\mathfrak{P}}$ der Fall ist. Somit ist $\left[\mathfrak{P}_Z, \overline{\mathfrak{P}}\right]$ ein Primideal 1. Relativgrades nach k dieses Kompositums. Da nun $(K_Z, \overline{K})$ nach dem schon Bemerkten zwischen K_Z und K_T liegt, muß notwendig $(K_Z, \overline{K}) = K_Z$, d. h. $\overline{K} \prec K_Z$ sein. Denn sonst wäre $(K_Z, \overline{K})$ einer der relativ zu K_Z zyklischen Zwischenkörper zwischen K_Z und K_T, in denen $\mathfrak{P}_Z$ notwendig seinen Grad erhöht, also keine Primteiler 1. Relativgrades besitzen kann.

3.18 Eine Arbeit von Tschebotareff. (9.10.1925)

Hasse works out the details of Chebotarev's paper [Tsc24]. *The aim is Satz 4 which gives a congruence condition for primes dividing the class number of a cyclotomic field, under certain conditions. Hasse had met Chebotarev recently at the annual meeting of the German Mathematical Society in Danzig, September 1925, and apparently Chebotarev had informed him about this result. Later Chebotarev had generalized this result on the suggestion of Hasse* [Tsc29]. *See also* [Met07] *and* [FR08], *section 11.3.1.*

III, 98

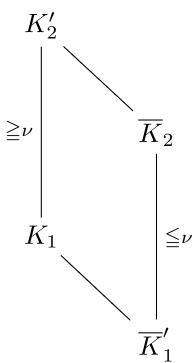
9. X. 1925

Satz 1. *Es sei K ein absolut–Galoisscher Körper. Dann ist das Kompositum aller Trägheitsgruppen von K die Galoissche Gruppe von K.*

Beweis: Nach Zahlbericht, Satz 76 ist eine Primzahl p dann und nur dann nicht in der Diskriminante eines Unterkörpers k von K enthalten, wenn alle Trägheitskörper zu p Oberkörper von k sind, wenn also alle Trägheitsgruppen zu p Untergruppen der Gruppe $\mathfrak{g}$ sind, zu der k gehört. Es sind also dann und nur dann alle p nicht in der Diskriminante von k enthalten, wenn alle Trägheitsgruppen von K Untergruppen von $\mathfrak{g}$ sind. Da nach Minkowski k dann und nur dann rational ist, wenn seine Diskriminante kein p enthält, ist also k dann und nur dann rational, wenn alle Trägheitsgruppen von K in $\mathfrak{g}$ enthalten sind, andererseits natürlich dann und nur dann, wenn $\mathfrak{g} = \mathfrak{G}$ ist. Somit sind dann und nur dann alle Trägheitsgruppen in $\mathfrak{g}$ enthalten, wenn $\mathfrak{g} = \mathfrak{G}$ ist, d. h. $\mathfrak{G}$ ist deren Kompositum. **Satz 2.** *Es sei K der Körper der ℓ^m–ten Einheitswurzeln (ℓ ungerade Primzahl), K_1 ein Unterkörper von K vom Grade n_1 und $\overline{K}_1$ ein Galoisscher, relativ zu K_1 Abelscher, unverzweigter Oberkörper von K_1. Ist dann $\mathfrak{N}$ ein in allen Trägheitsgruppen von $\overline{K}_1$ enthaltener Normalteiler der Galoisschen Gruppe $\mathfrak{G}$ von $\overline{K}_1$ von der Ordnung ν, so ist ν ein Teiler von n_1, und der zu $\mathfrak{N}$ gehörige Unterkörper $\overline{K}_2$ von $\overline{K}_1$ ist relativ–Abelsch, unverzweigt über dem Unterkörper K_2 von K_1 vom Grade $n_2 = \frac{n_1}{\nu}$ und es entsteht durch Komposition der relativ zu K_2 teilerfremden Körper K_1 und $\overline{K}_2$ der Körper $\overline{K}_1$.* III, 99

Beweis: Da ℓ in $\overline{K}_1$ in n_1–te Potenzen verschiedener Primideale zerfällt, haben die konjugierten Trägheitsgruppen von $\overline{K}_1$ die Ordnung n_1. Somit ist die Ordnung von $\mathfrak{N}$ ein Teiler ν von n_1. $\overline{K}_1$ ist über $\overline{K}_2$ vom Grade ν. Dies ν ist gleichzeitig die Relativordnung der Primteiler von ℓ in $\overline{K}_1$ nach $\overline{K}_2$. Denn jene Relativordnung ist die Ordnung des Durchschnittes $[\mathfrak{N}, \mathfrak{G}_T] = \mathfrak{N}$ von $\mathfrak{N}$ mit

einer Trägheitsgruppe von $\overline{K}_1$. Folglich haben die Primteiler von ℓ in $\overline{K}_2$ die Ordnung $\frac{n_1}{\nu} = n_2$. Somit hat der Durchschnitt $K_2' = \left[K_1, \overline{K}_2\right]$ höchstens den Grad n_2, es ist also der Grad von K_1 über K_2' *mindestens* ν. Andererseits ist der Grad von $\overline{K}_1' = (K_1, \overline{K}_2)$ über $\overline{K}_2$ *höchstens* gleich dem Grade ν von $\overline{K}_1$ über $\overline{K}_2$.



Nach dem Gradgesetz bei der Komposition von Galoisschen Körpern ist also der Wert beider Gradzahlen genau ν, d. h. es ist $K_2' = K_2$, $\overline{K}_1' = \overline{K}_1$, also

III, 100

$$K_2 = \left[K_1, \overline{K}_2\right], \ \overline{K}_1 = (K_1, \overline{K}_2).$$

Daraus folgt sofort der Rest der Behauptungen. Denn die Relativgruppe von $\overline{K}_2$ über K_2 ist bekanntlich isomorph zu der von $\overline{K}_1$ über K_1, also Abelsch, und $\overline{K}_2$ ist unverzweigt über K_2, weil schon im Unterkörper K_2 die Primteiler von ℓ die endgültige Ordnung n_2 erreichen.

Satz 3. *Ist in den Bezeichnungen von Satz 2 der Körper $\overline{K}_1$ der absolute Klassenkörper zu K_1, ferner $\mathfrak{N}$ der Durchschnitt aller Trägheitsgruppen zu $\overline{K}_1$, so ist $\overline{K}_2$ der absolute Klassenkörper zu K_2, und es ist K_2 der engste Unterkörper von K_1, dessen Klassenzahl gleich der von K_1 ist.*

Beweis: 1.) Nach Satz 2 hat $\overline{K}_2$ über K_2 denselben Relativgrad, wie $\overline{K}_1$ über K_1, also die Klassenzahl h_1 von K_1. Andererseits ist wegen Satz 2 jener Relativgrad Teiler der Klassenzahl h_2 von K_2. Also ist $h_1 | h_2$. Umgekehrt ist aber nach einem Satze von Furtwängler*) $h_2 | h_1$. Also ist $h_2 = h_1$, d. h. $\overline{K}_2$ der absolute Klassenkörper über K_2.

2.) Ist K_2' irgendein Unterkörper von K_1 mit der Klassenzahl h_1, so wäre nach

*) Vergl. dessen Verallgemeinerung in der folgenden Note.

dem Beweis des Furtwänglerschen Satzes [*)] für dessen absoluten Klassenkörper $\overline{K}_2'$:

$$K_2' = \left[K_1, \overline{K}_2'\right] \;; \quad \overline{K}_1 = (K_1, \overline{K}_2').$$

Ist nun $\mathfrak{N}'$ die $\overline{K}_2'$ als Unterkörper von $\overline{K}_1$ zugeordnete Gruppe, so ist die Ordnung ν' von $\mathfrak{N}'$ sowohl der Grad von $\overline{K}_1$ über $\overline{K}_2'$ als auch der von K_1 über K_2'. Da nun von $\overline{K}_2'$ nach $\overline{K}_1$ eine volle Verzweigung der Ordnung ν' eintreten muß, damit in $\overline{K}_1$ die Verzweigung der Ordnung n_1 zustandekommt, muß die Ordnung ν' von $\mathfrak{N}'$ gleichzeitig die Ordnung des Durchschnittes $[\mathfrak{N}', \mathfrak{G}_T]$ sein. Daraus folgt $\mathfrak{N}' \prec \mathfrak{G}_T$, d. h. $\mathfrak{N}' \prec \mathfrak{N}$. Es ist dann also ν' Teiler von ν, d. h. offenbar $K_2' \succ K_2$. Es existiert also ein engster Unterkörper von K_1, dessen Klassenzahl noch h_1 ist, und dieser ist gerade unser Körper K_2, dessen Klassenkörper $\overline{K}_2$ zum Trägheitsgruppendurchschnitt $\mathfrak{N}$ gehört.

III, 101

Satz 4. *Es sei K_1 ein Körper wie in Satz 2 vom Grade n_1 und der Klassenzahl h_1 und p eine Primzahl die in h_1, aber nicht in den Klassenzahlen der Teilkörper von K_1 aufgeht. Besitzt dann K_1 eine bei seinen Substitutionen invariante absolute Idealgruppe vom Index p, so ist*

$$p \equiv 1 \mod n_1.$$

Beweis: Nach den Voraussetzungen besitzt K_1 einen relativ–Abelschen, unverzweigten Oberkörper $\overline{K}_1$ vom Relativgrade p, der absolut–Galoissch ist, auf den also Satz 2 anwendbar ist. Ist also ν die Ordnung des Durchschnittes aller Trägheitsgruppen von $\overline{K}_1$, so existiert ein Unterkörper K_2 von K_1 vom Grade $\frac{n_1}{\nu}$, der einen relativ–Abelschen, unverzweigten Oberkörper vom Relativgrade p besitzt, dessen Klassenzahl also durch p teilbar ist. Nach der Voraussetzung muß dann $K_2 = K_1$, d. h. $\nu = 1$ sein. Die Trägheitsgruppen von $\overline{K}_1$ sind also teilerfremd. Ihre Ordnung ist n_1, und sie sind konjugierte Untergruppen der Galoisschen Gruppe $\mathfrak{G}$ von $\overline{K}_1$. $\mathfrak{G}$ besitzt demnach eine einstufig isomorphe Darstellung als Permutationsgruppe der Nebengruppen einer solchen Trägheitsgruppe $\mathfrak{G}_T$, deren Grad gleich dem Index von $\mathfrak{G}_T$, d. h. gleich $\frac{n_1 p}{n_1} = p$ ist. Da $\mathfrak{G}$ als Galoissche Gruppe eines auflösbaren Körpers auflösbar ist, ist jene Permutationsgruppe vom Primzahlgrade p linear, d. h. Teiler der vollen linearen Gruppe p–ten Grades, deren Ordnung $p(p-1)$ ist. Wegen der einstufigen Isomorphie hat dieser Teiler dieselbe Ordnung wie $\mathfrak{G}$, also die Ordnung pn_1. Daher ist $pn_1 | p(p-1)$, d. h. $n_1 | p-1$.

III, 102

Anwendung.

Satz 5. *Ist K_1 ein quadratischer Körper, dessen Diskriminante nur eine einzige ungerade Primzahl ℓ enthält, so ist die Klassenzahl von K_1 ungerade.*

Beweis: K_1 ist Unterkörper des Körpers der ℓ–ten Einheitswurzeln. Sei p ein Primfaktor der Klassenzahl von K_1. Dann ist Satz 4 auf diesen Fall anwendbar weil in K_1 für jede Idealklasse C gilt: $\sigma C = C^{-1}$ (wegen $C \cdot \sigma C = N(C) = 1$), III, 103 d. h. jede Idealgruppe von absoluten Idealklassen bei der erzeugenden Substitution σ von K_1 invariant bleibt. Also folgt $p \equiv 1 \mod 2$.

3.19 Die Idealklassengruppen relativ-Abelscher Körper. (10.10.1925)

Hasse derives a criterion for an abelian extension $K|k$ that the class number of k divides the class number of K. Furtwängler had shown that this is the case when K is a subfield of the ℓ^ν-th cyclotomic field [Fur08]. *Hasse's result here generalizes this for an arbitrary number field k, with the sole condition that the Hilbert class field of k is k-linearly disjoint to K. At the end of this entry Hasse refers to a later letter of Artin who had independently found the same criterion, even more general for arbitrary galois extensions $K|k$, not necessarily abelian. The criterion was rediscovered several times. See* [FR08], *section 11.3.1/2.*

III, 104

10. X. 25.

(Verallgemeinerung eines Satzes von Furtwängler).

Satz 1. *Es sei k ein beliebiger algebraischer Körper, K ein relativ–Abelscher Körper über k vom Relativgrad n, h und H die Klassenzahlen von k und K und $\overline{k}$ und $\overline{K}$ die absoluten Klassenkörper im weiteren (oder engeren) Sinne zu k und K. Wenn dann $\left[\overline{k}, K\right] = k$ ist, so ist $\overline{k} \prec \overline{K}$, und $h|H$.*

Beweis: Wir betrachten den Körper $\overline{K}' = (\overline{k}, K)$, der nach der Voraussetzung relativ–Abelsch vom Grade nh über K ist. Um zu zeigen, daß $\overline{K}'$ Unterkörper von $\overline{K}$ ist, woraus die Behauptungen folgen, betrachten wir die durch

$$N_{K,k}(\mathfrak{A}) = (\alpha)\,, \quad (\text{wo } \alpha \text{ total positiv})$$

definierte absolute Idealgruppe $\mathfrak{H}'_K$ in K. Ihr Index ist gleich der Anzahl der weiteren (engeren) Idealklassen in k, die Relativnormen aus K enthalten. Nun sei $\mathfrak{H}_k^{(0)}$ die Idealgruppe der (α) (wo α total positiv) in k, $\mathfrak{H}_k$ diejenige Idealgruppe mod. m, nach der K Klassenkörper zu k ist. Nach Voraussetzung ist dann $\left(\mathfrak{H}_k^{(0)}, \mathfrak{H}_k\right)$ die Gruppe aller Ideale aus k. Jedes (zu m prime) Ideal aus k ist daher einem Ideal aus $\mathfrak{H}_k$ im weiteren (engeren) Sinne äquivalent, d. h. in jeder weiteren (engeren) Idealklasse aus k gibt es Ideale aus $\mathfrak{H}_k$, also nach dem Satz von der arithmetischen Progression auch Primideale aus $\mathfrak{H}_k$, d. h. Relativnormen aus K. Daher ist der Index von $\mathfrak{H}'_K$ gleich h und die zugehörige Klassengruppe einstufig isomorph zur Idealklassengruppe im weiteren (engeren) Sinne von k.

III, 105

Nun liegen die Relativnormen aus $\overline{K}'$ nach K sämtlich in $\mathfrak{H}_K$, denn ihre Relativnormen nach k sind als Relativnormen von $\overline{K}'$ nach k auch Relativnormen aus $\overline{k}$, also in $\mathfrak{H}_k^{(0)}$. Daher ist der Index der $\overline{K}'$ in K mod. 1 zugeordneten Idealgruppe im weiteren (engeren) Sinne $\geqq h$, also $\geqq$ dem Relativgrad von $\overline{K}'$ über K. Daraus folgt, daß jener Index $= h$, also $\mathfrak{H}'_K$ die $\overline{K}'$ zugeordnete Idealgruppe mod. 1 und somit $\overline{K}'$ Klassenkörper zu jener Idealgruppe sein muß. Weil $\mathfrak{H}'_K$ die Gruppe $\mathfrak{H}_K^{(0)}$ aller Hauptideale von K im weiteren (engeren) Sinne enthält, ist dann $\overline{K}'$ in $\overline{K}$ enthalten. Damit ist der Satz bewiesen.

III, 106 **Satz 2.** *Unter den Voraussetzungen von Satz 1 „zerfällt“ jede Idealklasse c von k in K in $\frac{H}{h}$ Idealklassen C mit $N_{K,k}(C) = c$.*

Beweis: Das stellt nur eine andere Ausdrucksweise für die oben bewiesene Tatsache dar, daß die Klassengruppe nach $\mathfrak{H}'_K$ in K zu der nach $\mathfrak{H}_k^{(0)}$ in k einstufig isomorph ist.

Zusatz. *Ist speziell $(n, h) = 1$, so ist die Voraussetzung $\left[\overline{k}, K\right] = k$ von Satz 1 realisiert. Dann liefern die Idealklassen von k beim Übergang zu K eine einstufig isomorphe Untergruppe der Idealklassengruppe von K.*

Beweis: Das ist trivial. Denn aus $\mathfrak{a} \sim \mathfrak{b}$ in K folgt dann durch Relativnormbildung $\mathfrak{a}^n \sim \mathfrak{b}^n$ in k, also $\mathfrak{a} \sim \mathfrak{b}$ in k.

Ist aber $(n, h) \neq 1$, so kann „der Hauptkomplex“ in K sehr wohl „reduziert“ werden, d. h. in eine engere Klassengruppe in K als in k übergehen. Stets jedoch enthält die Klassengruppe von K eine zu der von k isomorphe Faktorgruppe, (wobei der Isomorphismus durch Satz 2 dargestellt ist), also bekanntlich auch eine zu der von k isomorphe Untergruppe, die aber nicht mit dem Hauptkomplex zusammenzufallen braucht.

Siehe auch Brief von Artin vom 26. VII. 27.

Kapitel 4

Tagebuch IV: Oktober 1925 – Sept. 1927

Eintragungen

4.1 Vier Theoreme der (12.10.1925 und 25.9.1927)

This entry contains 4 theorems belonging to the foundation of probability theory. He refers to the book of Hack [Hac11] *on probability theory but he criticizes the exposition there. We see that the entry carries two dates: the first is October 12, 1925 in line with the other entries of this notebook, and the second is September 25, 1927. It appears that at the later date Hasse had changed several statements in this entry but it is not evident which corrections have been made. We remark that in September 1927 Hasse prepared a paper (jointly with Tornier) in which he tried to apply probability arguments to density problems in algebraic number fields. See* [HT28].

IV, 3

(Exakt ausgearbeitet nach der schlechten Darstellung
bei *Hack* (Slg. Göschen), 12. X. 25 und 25. IX. 27)

1.) Das Theorem von J. Bernoulli.

Es seien E, F zwei einander ausschließende Ereignisse mit den Wahrscheinlichkeiten a priori p, q $(p+q=1)$. Dann sind für die Wahrscheinlichkeiten a posteriori $\frac{x}{n}, \frac{\beta}{n}$, wo bei n–maligem Versuch E in α, F in β Fällen eingetroffen ist $(\alpha+\beta=n)$, die Werte $\frac{\alpha_0}{n}=p$, $\frac{\beta_0}{n}=q$ die Wahrscheinlichkeiten.[1]

Die Wahrscheinlichkeit, daß die Wahrscheinlichkeiten a posteriori in den Grenzen

$$\left|\frac{\alpha}{n}-p\right|<\frac{\varepsilon\lg n}{\sqrt{n}},\quad \left|\frac{\beta}{n}-q\right|<\frac{\varepsilon\lg n}{\sqrt{n}}$$

bleiben, ist

$$w_{-\varepsilon}^{+\varepsilon}(n)=G\left(\frac{\varepsilon\lg n}{\sqrt{2pq}}\right)+O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

wo $G(x)=\frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}dt$ die Gausssche Fehlerfunktion ist.

Beweis: a.) Die Wahrscheinlichkeit, daß bei n–maligem Versuch E in α, F in β Fällen eintritt, ist nach dem Multiplikations– und dem Additionstheorem

$$w(\alpha,\beta)=\frac{n!}{\alpha!\beta!}p^\alpha q^\beta.$$

[1] Anm. d. Hrsg.: Bei den „Wahrscheinlichkeiten a posteriori“ handelt es sich wohl um das, was man heute „relative Häufigkeiten“ nennt.

Daraus folgt

$$w(\alpha+1,\beta-1) = \frac{\beta}{\alpha+1}\,\frac{p}{q} w(\alpha,\beta)$$

IV, 4 Daraus geht hervor, daß $w(\alpha,\beta)$ mit wachsendem α wächst, solange

$$\frac{\beta}{\alpha+1}\,\frac{p}{q} \geqq 1, \quad \beta p \geqq \alpha q + q$$

oder nach Addition von αp

$$np \geqq \alpha + q, \quad \alpha \leqq np - q$$

ist, und mit wachsendem α fällt, solange

$$\alpha \geqq np - q$$

ist. Die Umkehrstelle ist durch

$$\alpha_0 \geqq np - q, \quad \alpha_0 - 1 \leqq np - q$$

d. h.

$$np - q \leqq \alpha_0 \leqq np + p$$

charakterisiert. Hierdurch ist α_0 höchstens zweideutig, für hinreichend hohes n sogar sicher eindeutig, charakterisiert, und zwar ist

$$\frac{\alpha_0}{n} = p + \frac{\xi}{n}\,, \quad \frac{\beta_0}{n} = q - \frac{\xi}{n}$$
$$|\xi| \leqq 1.$$

Das ist der (hinsichtlich der notwendigen Ganzzahligkeit von α_0, β_0) genauere Sinn der ersten Aussage des Satzes.

b.) Wir setzen jetzt

$$\frac{\alpha}{n} = p + \frac{\lambda}{\sqrt{n}}\,, \quad \frac{\beta}{n} = q - \frac{\lambda}{\sqrt{n}}\,.$$

Dann ist nach dem Additionstheorem

$$w^{+\varepsilon}_{-\varepsilon}(n) = \sum_{|\lambda|<\varepsilon \lg n} w(\alpha,\beta),$$

wo über alle ganzzahligen Wertepaare α, β mit $|\lambda| < \varepsilon \lg n$ zu summieren ist. IV, 5
Um diese Summe in ein Integral zu verwandeln, benutzen wir die Stirlingsche Formel

$$n! = \sqrt{2\pi n}\, n^n e^{-n} \left(1 + O\Big(\frac{1}{n}\Big)\right).$$

Aus ihr ergibt sich

$$\begin{aligned}
\alpha! &= \sqrt{2\pi(pn+\lambda\sqrt{n})}(pn+\lambda\sqrt{n})^{pn+\lambda\sqrt{n}} e^{-pn-\lambda\sqrt{n}} \left(1 + O\Big(\frac{\lg n}{n}\Big)\right) \\
&= \sqrt{2\pi pn}(pn)^{pn} \left(1 + \frac{\sqrt{\lambda}}{p\sqrt{n}}\right)^{pn} (pn)^{\lambda\sqrt{n}} \left(1 + \frac{\lambda}{p\sqrt{n}}\right)^{\lambda\sqrt{n}} \\
&\quad \cdot e^{-pn} e^{-\lambda\sqrt{n}} \left(1 + O\Big(\frac{\lg n}{\sqrt{n}}\Big)\right).
\end{aligned}$$

Nun ist

$$\lg \left(1 + \frac{\lambda}{p\sqrt{n}}\right)^{pn} = pn \lg \left(1 + \frac{\lambda}{p\sqrt{n}}\right) = \lambda\sqrt{n} - \frac{\lambda^2}{2p} + O\left(\frac{\lg^3 n}{\sqrt{n}}\right),$$

also

$$\left(1 + \frac{\lambda}{p\sqrt{n}}\right)^{pn} = e^{\lambda\sqrt{n} - \frac{\lambda^2}{2p}} \left(1 + O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right),$$

ferner ähnlich

$$\left(1 + \frac{\lambda}{p\sqrt{n}}\right)^{\lambda\sqrt{n}} = e^{\frac{\lambda^2}{p}} \left(1 + O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right),$$

folglich

$$\begin{aligned}
\alpha! &= \sqrt{2\pi pn}(pn)^{pn} e^{\lambda\sqrt{n} - \frac{\lambda^2}{2p}} (pn)^{\lambda\sqrt{n}} e^{\frac{\lambda^2}{p}} e^{-pn} e^{-\lambda\sqrt{n}} \cdot \left(1 + O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right) \\
&= \sqrt{2\pi pn}(pn)^{pn} (pn)^{\lambda\sqrt{n}} e^{-pn} e^{\frac{\lambda^2}{2p}} \left(1 + O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right).
\end{aligned}$$

Ebenso ist IV, 6

$$\beta! = \sqrt{2\pi qn}(qn)^{qn}(qn)^{-\lambda\sqrt{n}}e^{-qn}e^{\frac{\lambda^2}{2q}}\left(1+O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right).$$

Damit wird

$$\begin{aligned}
w(\alpha,\beta) &= \frac{n!}{\alpha!\beta!}p^\alpha q^\beta \\
&= \frac{\sqrt{2\pi n}\,n^n e^{-n}p^{pn}p^{\lambda\sqrt{n}}q^{qn}q^{-\lambda\sqrt{n}}}{\sqrt{2\pi pn}(pn)^{pn}(pn)^{\lambda\sqrt{n}}e^{-pn}e^{\frac{\lambda^2}{pn}}\sqrt{2\pi qn}(qn)^{qn}(qn)^{-\lambda\sqrt{n}}e^{-qn}e^{\frac{\lambda^2}{2q}}}\cdot \\
&\quad \cdot\left(1+O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right) \\
&= \frac{1}{\sqrt{2\pi pqn}}e^{-\frac{\lambda^2}{2}\left(\frac{1}{p}+\frac{1}{q}\right)}\left(1+O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right) \\
&= \frac{1}{\sqrt{2\pi pqn}}e^{-\frac{\lambda^2}{2pq}}\left(1+O\Big(\frac{\lg^3 n}{\sqrt{n}}\Big)\right) \\
&= \frac{1}{\sqrt{2\pi pqn}}e^{-\frac{\lambda^2}{2pq}}+O\left(\frac{\lg^3 n}{n}\right).
\end{aligned}$$

Wir haben also

$$w_{-\varepsilon}^{+\varepsilon}(n) = \frac{1}{\sqrt{2\pi pqn}}\sum_{|\lambda|<\varepsilon\lg n} e^{-\frac{\lambda^2}{2pq}} + \sum_{|\lambda|<\varepsilon\lg n} O\left(\frac{\lg^3 n}{n}\right),$$

zu summieren über alle ganzen

$$\alpha = pn+\lambda\sqrt{n} \quad \text{mit} \quad |\lambda|<\varepsilon\lg n$$

Daher ist zunächst

$$\begin{aligned}
\sum_{|\lambda|<\varepsilon\lg n} O\left(\frac{\lg^3 n}{n}\right) &= O\left(\frac{\lg^3 n}{n}\right) = \sum_{|\lambda|<\varepsilon\lg n} 1 = O\left(\frac{\lg^3 n}{n}\right)O(\sqrt{n}\lg n) \\
&= O\left(\frac{\lg^4 n}{\sqrt{n}}\right).
\end{aligned}$$

Wird ferner $\lambda\sqrt{n}=\nu$, also

$$\alpha = pn+\nu \quad \text{mit} \quad |\nu|<\varepsilon\sqrt{n}\lg n$$

gesetzt, so wird IV, 7

$$w_{-\varepsilon}^{+\varepsilon}(n) = \frac{1}{\sqrt{2\pi pqn}} \sum_{|\nu|<\varepsilon\sqrt{n}} e^{-\frac{\nu^2}{2pqn}} + O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

wo ν eine Zahlenfolge mit den Abständen 1 in den genannten Grenzen durchläuft. Wir setzen nun

$$f(x) = e^{-\frac{x^2}{2pqn}}$$

und bilden für (nicht notw. ganzzahliges) ν mit $|\nu| < \varepsilon\sqrt{n}\lg n$

$$\begin{aligned} R_\nu &= \int_\nu^{\nu+1} f(x)\,dx - \left(\frac{f(\nu+1)+f(\nu)}{2}\right) \\ &= \int_0^1 f(\nu+t)\,dt - \int_0^1 \Big[f(\nu) + t\big(f(\nu+1) - f(\nu)\big)\Big]\,dt \\ &= \int_0^1 t\big[f'(\nu+\tau_1) - f'(\nu+\tau_2)\big]\,dt, \end{aligned}$$

wo τ_1, τ_2 Zahlen zwischen 0 und 1 sind. Da nun

$$\begin{aligned} \big|f'(\nu+\tau_1) - f'(\nu+\tau_2)\big| &= \big|\tau_1 - \tau_2\big|\big|f''(\nu+\tau_3)\big| \\ &\leqq \big|f''(\nu+\tau_3)\big| \end{aligned}$$

ist, wo τ_3 zwischen τ_1 und τ_2 liegt, so wird jedenfalls

$$|R_\nu| \leqq \frac{1}{2}\mathrm{Max}|f''(x)|.$$

Nun ist

$$f'(x) = -\frac{x}{pqn} f(x), \quad f''(x) = \left(\frac{x^2}{p^2q^2n^2} - \frac{1}{pqn}\right) f(x)$$

und für $|x| < \varepsilon\sqrt{n}\lg n$ somit, wegen $0 < f(x) < 1$:

$$f''(x) = O\left(\frac{\lg^2 n}{n}\right).$$

Daraus folgt IV, 8

$$R_\nu = O\left(\frac{\lg^2 n}{n}\right)$$

und somit, wenn ν_a und ν_b die Grenzwerte von ν bezeichnen,

$$\begin{aligned}
\int_{\nu_a}^{\nu_b} f(x)\,dx &= \sum_{\nu=\nu_a}^{\nu=\nu_b-1} \frac{f(\nu+1)+f(\nu)}{2} + O\left(\frac{\lg^3 n}{\sqrt{n}}\right) \\
&= \frac{f(\nu_0)}{2} + f(\nu_a+1) + \cdots + f(\nu_b-1) + \frac{f(\nu_b)}{2} + O\left(\frac{\lg^3 n}{\sqrt{n}}\right) \\
&= \sum_{\nu=\nu_a}^{\nu=\nu_b} f(\nu) + O(1),
\end{aligned}$$

und da ν_a von $-\varepsilon\sqrt{n}\lg n$, ν_b von $+\varepsilon\sqrt{n}\lg n$ höchstens um 1 abweichen,

$$\int_{-\varepsilon\sqrt{n}\lg n}^{+\varepsilon\sqrt{n}\lg n} f(x)\,dx = \sum_{|\nu|<\varepsilon\sqrt{n}\lg n} f(\nu) + O(1),$$

$$w_{-\varepsilon}^{+\varepsilon}(n) = \frac{1}{\sqrt{2\pi pqn}} \int_{-\varepsilon\sqrt{n}\lg n}^{+\varepsilon\sqrt{n}\lg n} e^{-\frac{x^2}{2pqn}}\,dx + O\left(\frac{\lg^4 n}{\sqrt{n}}\right).$$

Durch $\frac{x}{\sqrt{2pqn}} = t$ wird jetzt

$$w_{-\varepsilon}^{+\varepsilon}(n) = \frac{2}{\sqrt{\pi}} \int_0^{\frac{\varepsilon\lg n}{\sqrt{2pq}}} e^{-t^2}\,dt + O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

IV, 9 wie behauptet.

2.) Das Gesetz der großen Zahlen.

Zu jedem $\delta > 0$ und jedem $\varepsilon > 0$ existiert ein $n_0(\delta,\varepsilon)$, sodaß die Wahrscheinlichkeit dafür, daß die Wahrscheinlichkeiten a posteriori $\frac{\alpha}{n}, \frac{\beta}{n}$ von den Wahrscheinlichkeiten a priori p, q um weniger als $\frac{\varepsilon\lg n}{\sqrt{n}}$ abweichen:

$$\left|\frac{\alpha}{n} - p\right| < \frac{\varepsilon\lg n}{\sqrt{n}}\,, \quad \left|\frac{\beta}{n} - q\right| < \frac{\varepsilon\lg n}{\sqrt{n}}\,,$$

größer als $1-\delta$ ist, wenn nur die Versuchszahl $n \geqq n_0$ gewählt wird.

Das folgt unmittelbar aus dem Bernoullischen Theorem, weil bekanntlich

$$\lim_{x\to+\infty} G(x) = 1,$$

also bei jedem festen $\varepsilon > 0$

$$\lim_{n\to\infty} G\left(\frac{\varepsilon \lg n}{\sqrt{2pq}}\right) = 1$$

ist.

Bemerkung: Im Gesetz der großen Zahlen sind p, q als fest gegeben gedacht. Die Wahrscheinlichkeit bezieht sich auf $\frac{\alpha}{n}, \frac{\beta}{n}$ in einer Anzahl von Versuchsreihen, deren jede eine Länge $n \geqq n_0$ hat.

3.) Das Theorem von Bayes.

IV, 10

Es seien E, F zwei einander ausschließende Ereignisse mit den durch n–maligen Versuch festgestellten Wahrscheinlichkeiten a posteriori $\frac{\alpha}{n}, \frac{\beta}{n}$ $(\alpha+\beta = n)$. Dann sind für die Wahrscheinlichkeiten a priori p, q $(p+q = 1)$ die Werte $p_0 = \frac{\alpha}{n}, q_0 = \frac{\beta}{n}$ die wahrscheinlichsten.

Die Wahrscheinlichkeit, daß die Wahrscheinlichkeiten a priori in den Grenzen

$$\left|p - \frac{\alpha}{n}\right| < \frac{\varepsilon \lg n}{\sqrt{n}}, \quad \left|q - \frac{\beta}{n}\right| < \frac{\varepsilon \lg n}{\sqrt{n}}$$

liegen, ist

$$W_{-\varepsilon}^{+\varepsilon}(n) = G\left(\frac{\varepsilon \lg n}{\sqrt{2p_0q_0}}\right) + O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

wo

$$G(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2}\, dt$$

die Gausssche Fehlerfunktion ist.

Beweis: Nimmt man zunächst an, daß für p nur die Werte $\frac{\nu}{r}$ $(\nu = 0, \ldots, r)$ möglich und alle gleich wahrscheinlich seien, so ist die Wahrscheinlichkeit für einen bestimmten solchen Wert $\frac{1}{r+1}$ und die Wahrscheinlichkeit, daß dieser Wert $\frac{\nu}{r}$ vorliegt und daß dann die Reihe von n Versuchen α–mal E ergibt, nach dem

Multiplikationssatz $\frac{1}{r+1}\left(\frac{\nu}{r}\right)^{\alpha}\left(1-\frac{\nu}{r}\right)^{\beta}$. (Einer strengen Begründung scheint diese Anwendung des Multiplikationssatzes nicht fähig, vielmehr muß man es als Axiom genommen denken, daß man so ansetzen darf). Nach dem Additionssatz ist jetzt weiter die Wahrscheinlichkeit, daß $0 \leqq a \leqq p \leqq b \leqq 1$ ist und das genannte Versuchsergebnis resultiert,

IV, 11

$$\sum_{\nu} \frac{1}{r+1}\left(\frac{\nu}{r}\right)^{\alpha}\left(1-\frac{\nu}{r}\right)^{\beta}$$

wo $\frac{\nu}{r}$ alle Brüche vom Nenner r im Intervall $a \dots b$ durchläuft. Nimmt man nun an, daß p beliebig hohe Nenner haben kann, so wird die entsprechende Wahrscheinlichkeit der Grenzwert für $r \to \infty$, d. h.

$$\int_a^b p^{\alpha}(1-p)^{\beta} dp$$

Ebenso wird die Wahrscheinlichkeit, daß überhaupt, d. h. mit irgendeinem p, die Versuchsreihe α–mal E ergeben hat.

$$\int_0^1 p^{\alpha}(1-p)^{\beta} dp.$$

Nach dem Multiplikationssatz (strenge Begründung wieder anscheinend nicht möglich) ist aber jetzt die Wahrscheinlichkeit, daß zunächst dieser Tatbestand vorliegt und daß dann $a \leqq p \leqq b$ gewesen sei, gleich der Wahrscheinlichkeit, daß das Versuchsergebnis unter der Grundwahrscheinlichkeit $a \leqq p \leqq b$ zustande gekommen ist:

$$\int_0^1 p^{\alpha}(1-p)^{\beta} dp \cdot W_a^b = \int_a^b p^{\alpha}(1-p)^{\beta} dp,$$

also

$$W_a^b = \frac{\int_a^b p^{\alpha}(1-p)^{\beta} dp}{\int_0^1 p^{\alpha}(1-p)^{\beta} dp}.$$

Nimmt man diese Deduktion axiomatisch hin, so ist das folgende exakt.

IV, 12

a.) Am wahrscheinlichsten ist hiernach derjenige Wert von p, für den die Ele-

mentarwahrscheinlichkeit

$$\frac{p^\alpha(1-p)^\beta dp}{\int_0^1 p^\alpha(1-p)^\beta dp}$$

möglichst groß wird. Differentiiert man $p^\alpha(1-p)^\beta$ nach p, so erhält man (von den Grenzstellen $p = 0, p = 1$ abgesehen, wo ein Minimum 0 vorliegt)

$$p_0 = \frac{\alpha}{\alpha+\beta} = \frac{\alpha}{n}$$

als Extremum, das man leicht als Maximum erkennt.

b.) Wir berechnen zunächst das Nenner–Integral:

$$\begin{aligned}
\int_0^1 p^\alpha(1-p)^\beta dp &= (1-p)^\beta \frac{p^{\alpha+1}}{\alpha+1}\bigg|_0^1 + \frac{\beta}{\alpha+1}\int_0^1 p^{\alpha+1}(1-p)^{\beta-1}dp \\
&= \frac{\beta}{\alpha+1}\int_0^1 p^{\alpha+1}(1-p)^{\beta-1}dp \\
&= \frac{\beta\cdot(\beta-1)\cdots 1}{(\alpha+1)\cdot(\alpha+2)\cdots n}\int_0^1 p^n dp \\
&= \frac{1}{n+1}\cdot\frac{1}{\binom{n}{\beta}} = \frac{1}{n+1}\,\frac{\alpha!\beta!}{n!}
\end{aligned}$$

Folglich ist die im Satz genannte Wahrscheinlichkeit

$$W_{-\varepsilon}^{+\varepsilon}(n) = \frac{\int_{p_0-\varepsilon\frac{\lg n}{\sqrt{n}}}^{p_0+\varepsilon\frac{\lg n}{\sqrt{n}}} p^\alpha(1-p)^\beta dp}{\int_0^1 p^\alpha(1-p)^\beta dp} = (n+1)\frac{n!}{\alpha!\beta!}\int_{p_0-\varepsilon\frac{\lg n}{\sqrt{n}}}^{p_0+\varepsilon\frac{\lg n}{\sqrt{n}}} p^\alpha(1-p)^\beta dp.$$

IV, 13

$$\begin{aligned}
W_{-\varepsilon}^{+\varepsilon}(n) &= (n+1)\frac{n!}{\alpha!\beta!}\frac{\lg n}{\sqrt{n}}\int_{-\varepsilon}^{+\varepsilon}\left(p_0 + t\frac{\lg n}{\sqrt{n}}\right)^\alpha\left(q_0 - t\frac{\lg n}{\sqrt{n}}\right)^\beta dt \\
&= \frac{\lg n}{\sqrt{n}}(n+1)\frac{n!}{\alpha!\beta!}p_0^\alpha q_0^\beta\int_{-\varepsilon}^{+\varepsilon}\left(1+\frac{t}{p_0}\,\frac{\lg n}{\sqrt{n}}\right)^\alpha\left(1-\frac{t}{q_0}\,\frac{\lg n}{\sqrt{n}}\right)^\beta dt.
\end{aligned}$$

Wir haben nun

$$\begin{aligned}
n! &= \sqrt{2\pi n}\, n^n e^{-n} \left(1 + O(\frac{1}{n})\right) \\
p_0^\alpha &= p_0^{p_0 n} \\
q_0^\beta &= q_0^{q_0 n} \\
\alpha! &= \sqrt{2\pi\alpha}\, \alpha^\alpha e^{-\alpha} \left(1 + O(\frac{1}{n})\right) \\
&= \sqrt{2\pi p_0 n}(p_0 n)^{p_0 n} e^{-p_0 n} \left(1 + O(\frac{1}{n})\right) \\
\beta! &= \sqrt{2\pi q_0 n}(q_0 n)^{q_0 n} e^{-q_0 n} \left(1 + O(\frac{1}{n})\right),
\end{aligned}$$

also für den Ausdruck vor dem Integral:

$$\frac{\lg n}{\sqrt{n}}(n+1)\frac{n!}{\alpha!\beta!}p_0^\alpha q_0^\beta = \frac{\lg n}{\sqrt{n}}(n+1)\frac{1}{\sqrt{2\pi p_0 q_0 n}}\left(1 + O(\frac{1}{n})\right) = O(\lg n)$$

Ferner ist

$$\begin{aligned}
\lg\left(1 + \frac{t}{p_0}\frac{\lg n}{\sqrt{n}}\right)^\alpha &= p_0 n \left(\frac{t}{p_0}\frac{\lg n}{\sqrt{n}} - \frac{t^2 \lg^2 n}{2p_0^2 n} + O(\frac{\lg^3 n}{\sqrt{n}^{\,3}})\right) \\
&= t\sqrt{n}\lg n - \frac{t^2}{2p_0}\lg^2 n + O\left(\frac{\lg^3 n}{\sqrt{n}}\right) \\
\lg\left(1 - \frac{t}{q_0}\frac{\lg n}{\sqrt{n}}\right)^\beta &= -t\sqrt{n}\lg n - \frac{t^2}{2q_0}\lg^2 n + O\left(\frac{\lg^3 n}{\sqrt{n}}\right) \\
\lg\left[\left(1 + \frac{t}{p_0}\frac{\lg n}{\sqrt{n}}\right)^\alpha \left(1 - \frac{t}{q_0}\frac{\lg n}{\sqrt{n}}\right)^\beta\right] &= -\frac{t^2}{2p_0 q_0}\lg^2 n + O\left(\frac{\lg^3 n}{\sqrt{n}}\right).
\end{aligned}$$

IV, 14

$$\begin{aligned}
\left(1 + \frac{t}{p_0}\frac{\lg n}{\sqrt{n}}\right)^\alpha \left(1 - \frac{t}{q_0}\frac{\lg n}{\sqrt{n}}\right)^\beta &= e^{-\frac{t^2}{2p_0 q_0}\lg^2 n}\left(1 + O(\frac{\lg^3 n}{\sqrt{n}})\right) \\
&= e^{-\frac{t^2}{2p_0 q_0}\lg^2 n} + O\left(\frac{\lg^3 n}{\sqrt{n}}\right),
\end{aligned}$$

weil der vordere Faktor < 1 ist. Da nun der Faktor vor dem Integral $O(\lg n)$ ist, kommt bei Vernachlässigung des Restes unter dem Integral ein Fehlerglied

$O\left(\frac{\lg^4 n}{\sqrt{n}}\right)$. Somit folgt

$$W_{-\varepsilon}^{+\varepsilon}(n) = \frac{\lg n}{\sqrt{n}} \frac{n+1}{\sqrt{2\pi p_0 q_0 n}} \left(1 + O(\frac{1}{n})\right) \int_{-\varepsilon}^{+\varepsilon} e^{-\frac{t^2}{2p_0q_0}\lg^2 n} dt + O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

und weil das Integral selbst $O(1)$ ist, kann $O\left(\frac{1}{n}\right)$ in das letzte Fehlerglied gezogen werden, ebenso auch n statt $n+1$ geschrieben werden. Also folgt

$$W_{-\varepsilon}^{+\varepsilon}(n) = \frac{\lg n}{\sqrt{2\pi p_0 q_0}} \int_{-\varepsilon}^{+\varepsilon} e^{-\frac{t^2}{2p_0q_0}\lg^2 n} dt + O\left(\frac{\lg^4 n}{\sqrt{n}}\right).$$

Wird jetzt die Integrationsvariable geeignet transformiert, so kommt

$$W_{-\varepsilon}^{+\varepsilon}(n) = \frac{2}{\sqrt{\pi}} \int_0^{\frac{\varepsilon \lg n}{\sqrt{2p_0q_0}}} e^{-t^2} dt + O\left(\frac{\lg^4 n}{\sqrt{n}}\right),$$

wie behauptet.

4.) Die Umkehrung des Gesetzes der großen Zahlen.

IV, 15

Zu jedem $\delta > 0$ und jedem $\varepsilon > 0$ existiert ein $n_0(\delta, \varepsilon)$, sodaß die Wahrscheinlichkeit dafür, daß die Wahrscheinlichkeiten a priori p, q von den Wahrscheinlichkeiten a posteriori $\frac{\alpha}{n}, \frac{\beta}{n}$ um weniger als $\frac{\varepsilon \lg n}{\sqrt{n}}$ abweichen:

$$\left|p - \frac{\alpha}{n}\right| < \frac{\varepsilon \lg n}{\sqrt{n}}, \quad \left|q - \frac{\beta}{n}\right| < \frac{\varepsilon \lg n}{\sqrt{n}},$$

größer als $1 - \delta$ ist, wenn nur eine Versuchszahl $n \geqq n_0$ vorliegt.

Das folgt unmittelbar aus dem Bayesschen Theorem, weil

$$\lim_{n\to\infty} G\left(\frac{\varepsilon \lg n}{\sqrt{2p_0q_0}}\right) = 1$$

ist.

Bemerkung: In der Umkehrung des Gesetzes der großen Zahlen sind $\frac{\alpha}{n}, \frac{\beta}{n}$ als fest gegeben gedacht. Die Wahrscheinlichkeit bezieht sich auf p, q in einer Anzahl von Versuchsreihen, deren jede eine Länge $n \geqq n_0$ hat.

4.2 Über die Klassenzahl imaginär–quadratischer Körper. (13.10.1925)

On Dirichlet's class number formula for imaginary quadratic fields. See also the entry of April 1927.

IV, 16

(13. X. 25)

Es sei $p = 4n+3$ $(n > 0)$ eine positive Primzahl. Dann gilt für die Klassenzahl h von $R(\sqrt{-p})$ bekanntlich

$$\text{(I)} \qquad h = \frac{\sum b - \sum a}{p},$$

wo b alle $\frac{p-1}{2}$ kleinsten positiven quadratischen Nichtreste, a alle $\frac{p-1}{2}$ kleinsten positiven quadratischen Reste mod. p durchläuft. Ich beweise:

$$\text{(II)} \qquad h = \frac{(p-1)(p-2)}{6} - 2\sum_{\nu=1}^{n} [\sqrt{\nu p}\,].$$

Beweis: Aus

$$\sum b + \sum a = \sum_{\nu=1}^{p-1} \nu = \frac{p(p-1)}{2}$$

folgt zunächst

$$h = \frac{p-1}{2} - \frac{2}{p}\sum a.$$

(daß $\sum a \equiv 0 \mod. p$, folgt elementar aus

$$\sum a \equiv \sum_{\nu=1}^{\frac{p-1}{2}} \nu^2 = \frac{\frac{p-1}{2}\,\frac{p+1}{2}\,p}{6} \equiv 0 \mod. p\,, \quad \text{weil} \quad p > 3.$$

Die obige Formel zeigt übrigens auch die bekannte Tatsache $h \equiv 1 \mod. 2$).

Wir erzeugen nun die $\frac{p-1}{2}$ Zahlen a aus den $\frac{p-1}{2}$ inkongruenten quadratischen Resten $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ durch Subtraktion der entsprechenden Vielfachen von p. Wie man leicht nachrechnet, führt das zu

IV, 17

$$\begin{aligned}
\sum a &= \sum_{\nu=1}^{\frac{p-1}{2}} \nu^2 - \big([\sqrt{2p}] - [\sqrt{p}\,]\big)p - \big([\sqrt{3p}] - [\sqrt{2p}]\big)2p - \cdots \\
&\quad - \left(\frac{p-1}{2} - \left[\sqrt{\frac{p-3}{4}p}\right]\right)\frac{p-3}{4}p \\
\frac{\sum a}{p} &= \frac{(p-1)(p+1)}{24} + [\sqrt{p}\,] + \left[\sqrt{2p}\right] + \cdots \\
&\quad \cdots + \left[\sqrt{\frac{p-3}{4}p}\right] - \frac{(p-1)(p-3)}{8} \\
&= \frac{(p-1)(-p+5)}{12} + \sum_{\nu=1}^{n} [\sqrt{\nu p}\,]\,.
\end{aligned}$$

Durch Einsetzen in obige Formel gibt das die Behauptung (II). Ferner zeige ich:

(III) $$h = \frac{\sum b^2 - \sum a^2}{p^2}$$

Beweis: Da $\left(\frac{-1}{p}\right) = -1$ ist, erhält man die b als $p - a$. Folglich ist

$$\begin{aligned}
\sum b^2 - \sum a^2 &= \sum (p-a)^2 - \sum a^2 = \sum p^2 - 2p \sum a \\
&= p^2\,\frac{p-1}{2} - 2p\sum a = p^2\left(\frac{p-1}{2} - \frac{2}{p}\sum a\right) \\
&= p^2 h.
\end{aligned}$$

4.3 Zum Hilbertschen Hauptidealsatz. (27.9.1926)

Part of Furtwängler's work [Fur16] *on the capitulation of ideal classes in the unramified quadratic extensions of number fields with 2-class group of type* $(2;2)$ *is generalized to fields with* ℓ*-class group of type* (ℓ,ℓ)*: Hasse shows that the ideals from* k *with order* ℓ *capitulate in the Hilbert class field* K*.*

IV, 18

(Nach Ph. Furtwängler, Monatshefte für Math. u. Phys. XXVII (1916)).

(27. IX. 26).

Es sei ℓ eine Primzahl, k ein algebraischer Zahlkörper, dessen absolute Idealklassengruppe i. e. S. genau zwei Basiselemente der Ordnung ℓ (aber keine weiteren von Ordnungen ℓ^ν) enthält. Ferner sei K der Klassenkörper über k zur Idealgruppe der absoluten Idealklassen i. e. S. mit zu ℓ primen Exponenten, also K vom Typus (ℓ,ℓ) über k. Dann gilt:

Satz. *Die Ideale von* k *haben in* K *zu* ℓ *prime Exponenten i. e. S.*

Beweis: Es sei K_1 einer der in K enthaltenen relativ–zyklischen Körper ℓ–ten Grades über k. Dann ist nach der Klassenkörpertheorie die Anzahl der Geschlechter in K_1 gleich der Ordnung der Gruppe der ambigen Klassen in K_1 und gleich dem ℓ–ten Teil der Klassenzahl von k. Dabei kann, weil K_1 unverzweigt über k ist, das „Hauptgeschlecht in K_1" nach dem Strahl mod. p_∞ (abs. i. e. S.) erklärt werden, d. h. als die Gesamtheit der Strahlklassen mod. p_∞ in K_1, deren Relativnorm in den Strahl mod. p_∞ in k fallen. Die „ambigen Klassen in K_1" sind dann diejenigen Strahlklassen mod. p_∞ in K_1, die bei der erz. Subst. σ_1 von K_1/k invariant sind, und die „Klassenzahl von k" ist die Strahlklassenzahl mod. p_∞ von k*). Nach Voraussetzung ist die letztere genau durch ℓ^2 teilbar, sodaß also die Anzahl der Geschlechter in K_1 und die Anzahl der ambigen Klassen in K_1 beide genau durch ℓ teilbar sind. Da nun die Klassen von k in K_1 lauter ambige Klassen liefern, sind nur die folgenden beiden Fälle möglich:

IV, 19

a.) Die Klassen aus k liefern in K_1 lauter Klassen mit zu ℓ primem Exponenten.

b.) Die Klassen von k liefern in K_1 eine unabhängige Klasse vom Exponenten ℓ.

*) Im folgenden bedeutet „Klasse" stets „Strahlklasse mod. p_∞", d. h. „absolute Idealklasse i. e. S.".

Im Falle a.) gilt dasselbe erst recht in K, und der Beweis ist erbracht. Im Falle b.) bedenken wir, daß die Anzahl der ambigen Klassen von K/K_1 gleich dem ℓ–ten Teil der Klassenzahl von K_1 ist. Insbesondere muß daher die Klassengruppe von K_1 in K eine Reduktion auf einen Teil erfahren, der ein Multiplum von ℓ ist, d. h. die Gruppe derjenigen Klassen aus K_1, die in K die Hauptklasse werden, hat ein Multiplum von ℓ zur Ordnung. Daher gibt eine Klasse C_1 der Ordnung ℓ in K_1, sodaß $C_1 = 1$ in K wird. Da nun

$$(1-\sigma_1)^\ell = \ell\varphi(\sigma_1)$$

ist, ist

$$C_1^{(1-\sigma_1)^\ell} = 1 \quad \text{in} \quad K_1.$$

Sei dann n der kleinste Exponent, sodaß IV, 20

$$C_1^{(1-\sigma_1)^n} = 1 \quad \text{in} \quad K_1$$

ist, so ist jedenfalls $n \geqq 1$ nach Wahl von C_1. Für die Klasse $\overline{C}_1 = C_1^{(1-\sigma_1)^{n-1}}$ gilt dann:

$$\overline{C}_1 \neq 1 \quad \text{in} \quad K_1\,, \quad \overline{C}_1^{1-\sigma_1} = 1 \quad \text{in} \quad K_1\,, \quad \overline{C}_1 = 1 \quad \text{in} \quad K,$$

letzteres, weil K relativ–Galoissch über k, also $\sigma_1 K = K$ ist, sodaß mit C_1 auch $C_1^{g(\sigma)}$ in K die Hauptklasse ist. Natürlich hat auch $\overline{C}_1$ die Ordnung ℓ, weil $\overline{C}_1^\ell = C_1^{\ell(1-\sigma_1)^{n-1}} = 1$ in K_1, aber $\overline{C}_1 \neq 1$ in K_1 ist. Die Klasse $\overline{C}_1$ ist also eine ambige Klasse der Ordnung ℓ in K_1. Da aber die Anzahl der ambigen Klassen in K_1 genau durch ℓ teilbar ist, kann $\overline{C}_1$ als die in b.) genannte unabhängige Klasse verwendet werden, d. h. $\overline{C}_1$ wird schon durch eine Klasse aus k erzeugt. Da $\overline{C}_1 = 1$ in K ist, fallen dann nach b.) die Klassen aus k in die Hauptklasse in K, w. z. b. w.

4.4 Formeln für die Klassenzahl imaginär–quadratischer Körper. (April 1927)

Formulas to compute the class numbers of imaginary quadratic fields, according to the arithmetic properties of the discriminant. See also the entry of October 13, 1925.

IV, 21

(April 1927)

Es sei $d \neq -3, -4$ die Diskriminante eines imaginär–quadratischen Körpers. Dann ist seine Klassenzahl

$$h = \frac{1}{d} \sum_{n=1}^{|d|} \left(\frac{d}{n}\right) n.$$

Dabei ist

$$\left(\frac{d}{p}\right) = +1, -1, 0$$

entsprechend den 3 Zerlegungsformen von p.

Für die numerische Rechnung bequemer sind folgende Formeln in denen bezeichnet:

d_0 den ungeraden positiven Bestandteil von $d = -2^\delta d_0$ $(\delta = 0, 2, 3)$

n_i alle Zahlen $\equiv i \bmod. 2^\delta$ mit $1 \leqq n_i \leqq \frac{d_0 - 1}{2}$ und $(n_i, d_0) = 1$.

$h = \sum \left(\frac{n_1}{d_0}\right)$ für $d \equiv 1 \bmod. 8$

$h = \frac{1}{3} \sum \left(\frac{n_1}{d_0}\right)$ für $d \equiv 5 \bmod. 8$

$h = \sum \left[\left(\frac{n_1}{d_0}\right) - \left(\frac{n_2}{d_0}\right) - \left(\frac{n_3}{d_0}\right) + \left(\frac{n_4}{d_0}\right)\right]$ für $d = -2^2 d_0$, $d_0 \equiv 1 \bmod. 4$

$h = 2 \sum \left[\left(\frac{n_1}{d_0}\right) - \left(\frac{n_4}{d_0}\right) - \left(\frac{n_5}{d_0}\right) + \left(\frac{n_8}{d_0}\right)\right]$ für $d = -2^3 d_0$, $d_0 \equiv 1 \bmod. 8$

$h = 2 \sum \left[\left(\frac{n_1}{d_0}\right) + \left(\frac{n_4}{d_0}\right) - \left(\frac{n_5}{d_0}\right) - \left(\frac{n_8}{d_0}\right)\right]$ für $d = -2^3 d_0$, $d_0 \equiv 5 \bmod. 8$

$h = 2 \sum \left[\left(\frac{n_1}{d_0}\right) - \left(\frac{n_2}{d_0}\right) - \left(\frac{n_5}{d_0}\right) + \left(\frac{n_6}{d_0}\right)\right]$ für $d = -2^3 d_0$, $d_0 \equiv 3 \bmod. 8$

$h = 2 \sum \left[\left(\frac{n_1}{d_0}\right) + \left(\frac{n_2}{d_0}\right) - \left(\frac{n_5}{d_0}\right) - \left(\frac{n_6}{d_0}\right)\right]$ für $d = -2^3 d_0$, $d_0 \equiv 7 \bmod. 8$

Damit sind alle Möglichkeiten für d erschöpft.

4.5 Dyadische Lösung des Kirkmannschen Problems. (26.9.1927)

See also the entry of 2 May 1924 in Book III where Hasse had written down the solution of Kirkman's problem by Schreier.] There Hasse said that he did not know whether there may be other solutions. Now here he gives two different solutions. We observe that Hasse refers to his own notes from the year 1916. At that year Hasse was serving in the navy (it was war time). It seems that even during his days of military duty he had found time to work out mathematical problems.

IV, 22

(Nach Aufzeichnungen aus 1916)

(26. IX. 27).

1	2	3	1	4	5	1	6	7	1	8	9
4	8	12	2	13	15	2	8	10	2	12	14
5	10	15	3	9	10	3	12	15	3	5	6
6	11	13	6	8	14	4	9	13	4	11	15
7	9	14	7	11	12	5	11	14	7	10	13

1	10	11	1	12	13	1	14	15
2	4	6	2	5	7	2	9	11
3	13	14	3	8	11	3	4	7
5	9	12	4	10	14	5	8	13
7	8	15	6	9	15	6	10	12

Andere Lösung (nicht dyadisch)

1	2	3	1	4	5	1	6	7	1	10	11
4	9	15	2	8	10	2	9	11	2	13	15
5	11	12	3	12	15	3	13	14	3	5	6
6	10	14	6	9	13	4	10	12	4	8	14
7	8	13	7	11	14	5	8	15	7	9	12

1	8	9	1	12	13	1	14	15
2	12	14	2	4	6	2	5	7
3	4	7	3	8	11	3	9	10
5	10	13	5	9	14	4	11	13
6	11	15	7	10	15	6	8	12

4.6 Elementare Theorie der Funktion $x!$ im Anschluß an Gauss. (26.9.1927)

Elementary discussion of the Gamma function following Gauss. (The idea of evaluating a divergent series by summing it until the terms begin to diverge was often used by Euler.) This is a copy of a manuscript by Hermann Wolff, the school teacher of Hasse. That manuscript is dated by Hasse to the year 1915, which is the year when Hasse got his "Abitur" and left school. It appears that the young Hasse got that manuscript as a gift from his school teacher. Hasse kept friendship with his teacher throughout his life; the Hasse papers in Göttingen contain more than 200 letters from Wolff during the years 1915-1942. It appears that Hasse copied this manuscript since he had to lecture on the Gamma function in his course and he wished to recall Wolff's elementary treatment. Compare with Artin's completely different introductory treatment of the Gamma function [Art31] *which Artin also had written for use in his lectures, and which Artin sent to Hasse in 1931; see* [FR08].

IV, 23

(Nach einem Manuskript von H. Wolff, Sommer 1915)

(Wörtlich übertragen 26. IX. 27).

Für ganzzahlige positive x ist die Funktion $x!$ bekanntlich definiert durch das Produkt $1 \cdot 2 \cdot 3 \cdots x$. Um zu einer Erweiterung des Definitionsbereichs zu gelangen, schreiben wir jenen Ausdruck in der Form

$$x! = \frac{1 \cdot 2 \cdots n}{(x+1)(x+2)\cdots n},$$

wo n eine beliebige positive ganze Zahl $> x$ bedeutet, die also auch beliebig hoch sein kann. Diese Darstellung gibt für $x = 0$: $0! = 1$ und für $x = -1, -2, -3, \ldots$ ∞ von der ersten Ordnung.

Die gegebene Darstellungsweise versagt jedoch für gebrochene x. Denn der mit den nicht ganzzahligen Faktoren $x+1, x+2, \ldots$ beginnende Nenner kann nicht mit dem ganzzahligen n schließen.

Zur Beseitigung dieser Schwierigkeit betrachten wir obigen Quotienten zunächst wieder für ganzzahlige positive x, multiplizieren ihn mit $\frac{n^x}{(n+1)\cdots(n+x)}$ *und lassen n dann unendlich werden.* Hierdurch wird für ganzzahlige positive x nichts an obigem Quotienten geändert, denn für solche ist $\lim\limits_{n\to\infty} \frac{n^x}{(n+1)\cdots(n+x)} = 1$.

Zugleich ist aber der hervorgehende Ausdruck:

$$x! = \lim_{n\to\infty} \frac{n^x \cdot 1 \cdot 2 \cdots n}{(x+1)\cdots(x+n)}$$

nun auch für nicht ganzzahlige positive oder negative x (auch für komplexe x) definiert. Daß er für solche x konvergiert, wird später dadurch gezeigt, daß $\lg x!$ konvergiert. Für $x = 0$ ist er nach wie vor 1 und für $x = -1, -2, -3, \ldots$ ist er einfach unendlich. IV, 24

Diese Definition von $x!$ hat *Gauss* gefunden.[1] Was die Terminologie betrifft, so spricht er jedoch von der *Gamma–Funktion* $\Gamma(x)$ im Anschluß an *Legendre*. Für ganzzahlige positive x ist $\Gamma(x) = (x-1)!$. *Legendre* definiert $\Gamma(x)$ durch das bestimmte Integral

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt,$$

welches zugleich mit verwandten Integralen zuerst von *Euler*, später von zahlreichen Mathematikern untersucht wurde.

Erste Haupteigenschaft: $(x+1)! = x!(x+1)$.

Diese für ganzzahlige positive x wohlbekannte Eigenschaft beweisen wir, wie folgt: Es ist

$$\begin{aligned} (x+1)! &= \lim_{n\to\infty} \frac{n^{x+1}\, n!}{(x+2)\cdots(x+n+1)} \\ x! &= \lim_{n\to\infty} \frac{n^x\, n!}{(x+1)\cdots(x+n)}, \end{aligned}$$

also durch Division

$$\frac{(x+1)!}{x!} = \lim_{n\to\infty} \frac{n(x+1)}{x+n+1} = x+1.$$

Die erste Haupteigenschaft gibt den Verlauf von $x!$ in einem beliebigen Intervall von der Länge 1, wenn der Verlauf in *einem* solchen Intervall bekannt ist.

Zweite Haupteigenschaft: $x!(-x)! = \frac{\pi x}{\sin \pi x}$. IV, 25

[1] Anm. d. Hrsg.: Diese Definition findet sich schon im ersten Brief von Euler an Goldbach (13. Okto. 1729).

Beweis:

$$x! = \lim_{n\to\infty} \frac{n^x\, n!}{(x+1)\cdots(x+n)}$$

$$(-x)! = \lim_{n\to\infty} \frac{n^{-x}\, n!}{(-x+1)\cdots(-x+n)}\,.$$

Die Multiplikation beider Gleichungen gibt

$$x!(-x)! = \lim_{n\to\infty} \frac{(n!)^2}{(1^2-x^2)\cdots(n^2-x^2)}$$

oder durch Kürzen mit $(n!)^2$

$$= \lim_{n\to\infty} \frac{1}{\left(1-\frac{x^2}{1^2}\right)\cdots\left(1-\frac{x^2}{n^2}\right)}$$

$$= \frac{1}{\left(1-\frac{x^2}{1^2}\right)\left(1-\frac{x^2}{2^2}\right)\cdots}$$

Nun ist bekanntlich

$$\sin x = x\left(1-\frac{x^2}{\pi^2}\right)\left(1-\frac{x^2}{2^2\pi^2}\right)\cdots\,,$$

also

$$\sin \pi x = \pi x\left(1-\frac{x^2}{1^2}\right)\left(1-\frac{x^2}{2^2}\right)\cdots\,,$$

mithin

$$x!(-x)! = \frac{\pi x}{\sin \pi x}\,.$$

Diese zweite Haupteigenschaft gibt den Verlauf von $x!$ im Intervall $0\ldots-\frac{1}{2}$, wenn sie im Intervall $0\ldots+\frac{1}{2}$ bekannt ist, und reduziert somit (in Verbindung mit der ersten Haupteigenschaft) das Problem auf die Kenntnis von $x!$ in einem beliebigen Intervall von der Länge $\frac{1}{2}$.

Da $\lim\limits_{x\to 0} \frac{\pi x}{\sin \pi x} = 1$ ist, so sieht man noch, daß für sehr kleine x $x!$ und $(-x)!$ nahezu reziprok sind.

Wir machen eine Anwendung, indem wir $x = \frac{1}{2}$ setzen. Es wird $\frac{1}{2}!\,\left(-\frac{1}{2}\right)! = \frac{\pi}{2}$, und da nach der ersten Haupteigenschaft $\frac{1}{2}! = \left(-\frac{1}{2}\right)! \cdot \frac{1}{2}$ ist, so wird IV, 26

$$\left(-\tfrac{1}{2}\right)!^2 = \pi\,, \quad \left(-\tfrac{1}{2}\right)! = \sqrt{\pi}$$
$$\left(\tfrac{1}{2}\right)! = \tfrac{1}{2}\sqrt{\pi}$$
$$\left(-\tfrac{1}{2}\right)!\,\left(\tfrac{1}{2}\right)! = \tfrac{\pi}{2} \sim 1,5\,.$$

Reihenentwicklung für lg x! und numerische Auswertung der Funktion x!.

Logarithmiert man die Definitionsgleichung für x!, so erhält man

$$\lg x! = \lim_{n\to\infty} \big(x\lg n + \lg n! - \lg(x+1) - \cdots - \lg(x+n)\big).$$

Hieraus erhält man durch Differentiation*)

$$\begin{aligned}
\frac{d\lg x!}{dx} &= \lim_{n\to\infty}\left(\lg n - \frac{1}{x+1} - \cdots - \frac{1}{x+n}\right)\\
\frac{d^2\lg x!}{dx^2} &= \frac{1}{(x+1)^2} + \frac{1}{(x+2)^2} + \cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\frac{d^\mu\lg x!}{dx^\mu} &= (\mu-1)!(-1)^\mu\left(\frac{1}{(x+1)^\mu} + \frac{1}{(x+2)^\mu} + \cdots\right),
\end{aligned}$$

also für $x = 0$

$$\left.\frac{d^\mu\lg x!}{dx^\mu}\right|_{x=0} = (\mu-1)!(-1)^\mu\left(\frac{1}{1^\mu} + \frac{1}{2^\mu} + \cdots\right). \tag{1}$$

Diese Gleichung gilt aber, wie aus der Entwicklung zu entnehmen ist, nur für $\mu = 2, 3, 4, \ldots$, während für $\mu = 1$ ist:

$$\left.\frac{d\lg x!}{dx}\right|_{x=0} = \lim_{n\to\infty}\left(\lg n - \frac{1}{1} - \frac{1}{2} - \cdots\right). \tag{2}$$

Es läßt sich zeigen, daß sowohl die in (1) auftretende unendliche Reihe für $\mu = 2, 3, 4, \ldots$, als auch der in (2) auftretende Limes konvergieren†). Der entgegengesetzte Wert des letzteren heißt *Eulersche Konstante*. Sie ist definiert durch‡) IV, 27

$$C = \lim_{n\to\infty}\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} - \lg n\right)$$

---

*) Bem. b. d. Übertragung: *Sachlich* sind diese Differentiationen in Ordnung, nur *ungenügend motiviert*! Man bestätige sie rückwärts durch Integration!

†) Die Reihe $\frac{1}{1} + \frac{1}{2} + \cdots$ divergiert; sie heißt *harmonische Reihe*.

‡) Für ganzzahlige x ist auch $C = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{x} - \frac{d\lg x!}{dx}$ (endliche Reihe, s. *Serret–Scheffers S. 209*). (Beweis ohne weiteres nach voriger Seite!)

(Aus diesem Limes lassen sich merkwürdige Folgerungen über bedingt konvergente Reihen ziehen, s. *Weber–Riemann* Bd. I, S. 53).

$$C = 0,57721\,56649\,015328\ldots$$

Die Summen $S_\mu = \frac{1}{1^\mu} + \frac{1}{2^\mu} + \cdots$ sind von *Legendre* für $\mu = 2, \ldots, 35$ auf 16 Dezimalen angegeben.

Mit Benutzung der Zeichen C und S_μ und des Wertes $\lg 0! = 0$ wird die MacLaurinsche Reihe

$$f(x) = f(0) + f'(0)\frac{x}{1!} + f''(0)\frac{x^2}{2!} + \cdots$$

für die Funktion $\lg x!$

$$\lg x! = -Cx + S_2\frac{x^2}{2} - S_3\frac{x^3}{3} + \cdots \tag{3}$$

Das Verschwinden des Restgliedes ist leicht nachzuweisen. Die Reihe selbst löst im Prinzip das Problem der numerischen Auswertung der Funktion $\lg x!$ und durch Übergang zum Numerus das der Auswertung von $x!$ selbst.

Eine besser konvergierende Reihe erhält man, wenn man zu (3) die freilich nur im Intervall $|x| < 1$ gültige Reihe

$$0 = -\lg(x+1) + \frac{x}{1} - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

hinzufügt (Bem. b. d. Übertragung: (3) konvergiert auch nur im Intervall $|x| <$ 1). Dies ergibt

IV, 28

$$\lg x! = -\lg(x+1) + (1-C)x + \frac{S_2 - 1}{2}x^2 - \frac{S_3 - 1}{3}x^3 + \cdots. \tag{4}$$

Um die Konvergenz noch weiter zu verstärken, subtrahieren wir von (4) die Reihe

$$\lg(-x)! = -\lg(1-x) - (1-C)x + \frac{S_2 - 1}{2}x^2 + \frac{S_3 - 1}{3}x^3 + \cdots$$

und erhalten

$$\lg x! - \lg(-x)! = -\lg\frac{1+x}{1-x} + 2(1-C)x - 2\frac{S_3 - 1}{3}x^3 - 2\frac{S_5 - 1}{5}x^5 - \cdots$$

Nun ist nach der zweiten Haupteigenschaft

$$\lg x! + \lg(-x)! = \lg \frac{\pi x}{\sin \pi x}$$

Addiert man daher die beiden letzten Gleichungen und dividiert durch 2, so erhält man die im Intervall $|x| < 1$ gültige und im Intervall $0 < x < \frac{1}{2}$ sehr schnell konvergierende Reihe:

$$(5) \quad \lg x! = \frac{1}{2}\lg \frac{\pi x}{\sin \pi x} - \frac{1}{2}\lg \frac{1+x}{1-x} + (1-C)x - \frac{S_3 - 1}{3}x^3 - \frac{S_5 - 1}{5}x^5 - \cdots$$

Diese Reihe kann auch dazu dienen, die Konstante C aus $S_3, S_5, \ldots$ zu berechnen. Setzt man nämlich $x = 1$ und $x = \frac{1}{2}$ und beachtet, daß $\lg 1! = 0$ und $\lg\left(\frac{1}{2}\right)! = \lg \frac{1}{2}\sqrt{\pi}$ ist, und daß ferner $\lg \frac{\pi x}{\sin \pi x} + \lg(1-x)$ für $x = 1$ verschwindet, so hat man

$$\begin{aligned} 1 - C &= \frac{1}{2}\lg 2 + \frac{S_3 - 1}{3} + \frac{S_5 - 1}{5} + \cdots \\ 1 - C &= \lg \frac{3}{2} + \frac{S_3 - 1}{3}\frac{1}{2^2} + \frac{S_5 - 1}{5}\frac{1}{2^4} + \cdots \end{aligned}$$

Asymptotische Werte für $x!$ liefern für jedes positive x

$$\sqrt{2\pi x}x^x e^{-x} < x! < \sqrt{2\pi x}x^x e^{-x+\frac{1}{12x}}$$

(siehe *Serret–Scheffers*, S. 238), können auch aus der *Stirling*schen Reihe gefolgert werden (siehe ebenda, S. 251).

IV, 29

$$\begin{aligned} C &= 0,57721566\ldots \\ S_3 &= 1,20205690\ldots \\ S_5 &= 1,03692776\ldots \\ S_7 &= 1,00834928\ldots \\ S_9 &= 1,00200839\ldots \\ S_{11} &= 1,0005\ldots \\ S_{13} &= 1,00012\ldots \\ S_{15} &= 1,00003\ldots \\ S_{17} &= 1,00001\ldots \end{aligned}$$

Funktionentheoretischer Aufbau der Funktion $x!$

Vom funktionentheoretischen Standpunkt besitzt die nach S. 23] definierte Funktion $x!$ die Stellen $-1, -2, -3, \ldots$ zu einfachen Polen und das Unendliche als wesentliche Singularität. Die Funktion $\frac{1}{x!}$ hat daher $-1, -2, -3, \ldots$ zu einfachen Nullstellen, und gestattet somit als *ganze transzendente Funktion* die Weierstrasssche Produktentwicklung

$$\frac{1}{x!} = e^{G(x)} \prod_{n=1}^{\infty} \left[\left(1 + \frac{x}{n}\right) e^{-\frac{x}{n} + \frac{x^2}{2n^2} - \cdots \pm \frac{x^{\nu-1}}{(\nu-1)n^{\nu-1}}} \right],$$

wo ν so hoch zu bestimmen ist, daß

$$\sum_{n=1}^{\infty} \left(\frac{1}{x+n} - \frac{1}{n} + \frac{x}{n^2} - \cdots \pm \frac{x^{\nu-2}}{n^{\nu-1}} \right)$$

konvergiert. Es genügt *nicht*, $\nu - 1 = 0$ zu nehmen, da $\sum_{n=1}^{\infty} \frac{1}{x+n}$ bekanntlich divergiert. Wohl aber genügt es, $\nu - 1 = 1$ zu nehmen, denn es konvergiert $\sum_{n=1}^{\infty} \frac{1}{n^2}$ und also auch $\sum_{n=1}^{\infty} \left(\frac{1}{x+n} - \frac{1}{n} \right) = -x \sum_{n=1}^{\infty} \frac{1}{n^2} \frac{1}{1+\frac{x}{n}}$, da sämtliche IV, 30 Faktoren $\frac{1}{1+\frac{x}{n}}$ unter einer festen Grenze bleiben. Wir haben also in

$$\frac{1}{x!} = e^{G(x)} \prod_{n=1}^{\infty} \left[\left(1 + \frac{x}{n}\right) e^{-\frac{x}{n}} \right] \tag{1}$$

zunächst eine Funktion mit den gewünschten einfachen Nullstellen.

Die ganze transzendente Funktion $G(x)$ bestimmt sich nun aus den Bedingungen $x! = 1 \cdot 2 \cdots x$ für ganzzahliges x, wie folgt: Wir logarithmieren (1) und erhalten

$$\begin{aligned} -\lg x! &= G(x) - \sum_{n=1}^{\infty} \left[\frac{x}{n} - \lg \frac{n+x}{n} \right] \\ &= G(x) - \lim_{n\to\infty} \left[x \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} \right) - \right. \\ &\qquad \left. - \lg \frac{(x+1)\cdots(x+n)}{1 \cdots n} \right] \end{aligned} \tag{2}$$

Setzen wir nun an

$$G(x) = a_0 + a_1 x + a_2 x^2 + \cdots,$$

so erhalten wir für $x = 0$ aus (2): $G(0) = 0$ und daher

$$a_0 = 0,$$

für $x = 1$ aus (2):

$$0 = a_1 - \lim_{n\to\infty}\left[1 + \frac{1}{2} + \cdots + \frac{1}{n} - \lg(n+1)\right]$$
$$a_1 = C \qquad \text{(Eulersche Konstante)},$$

für $x = 2$ aus (2):

$$-\lg 2! = 2C + 2^2 a_2 + 2^3 a_3 + \cdots -$$
$$\lim_{n\to\infty}\left[2\left(1 + \frac{1}{2} + \cdots + \frac{1}{n}\right) - \lg\frac{(n+1)(n+2)}{1\cdot 2}\right]$$
$$-\lg 2! = 2C + 2^2 a_2 + 2^3 a_3 + \cdots - 2C - \lg 2!\,,$$

d. h.

$$0 = 2^2 a_2 + 2^3 a_3 + \cdots\,,$$

für $x = 3, 4, \ldots$ ebenso

$$0 = 3^2 a_2 + 3^3 a_3 + \cdots$$
$$0 = 4^2 a_2 + 4^3 a_3 + \cdots$$

Allen diesen Gleichungen genügt

$$a_2 = 0,\ a_3 = 0,\ a_4 = 0, \ldots$$

also IV, 31

$$G(x) = Cx\,,$$

und somit ist

$$\frac{1}{x!} = e^{Cx}\prod_{n=1}^{\infty}\left[\left(1 + \frac{x}{n}\right)e^{-\frac{x}{n}}\right] \tag{3}$$

die gesuchte ganze transzendente Funktion. Diese Entwicklungen lassen die nahe Verwandtschaft der ganzen transzendenten Funktionen $\frac{1}{x!}$ und $\sin \pi x$ erkennen. Letztere hat außer den Nullstellen von $\frac{1}{x!}$ noch $0, 1, 2, \ldots$ zu einfachen Nullstellen.

Aus (3) folgt

$$x! = e^{-Cx} \prod_{n=1}^{\infty} \frac{n}{x+n} e^{+\frac{x}{n}}.$$

Um die Identität dieses unendlichen Produktes mit dem Limes a. S. 23] auch formal darzutun, brauchen wir nur umzuordnen:

$$\begin{aligned} x! &= e^{\lim\limits_{n\to\infty}\left(x \lg n - \frac{x}{1} - \cdots - \frac{x}{n}\right)} \lim_{n\to\infty} \left[\frac{1 \cdot 2 \cdots n}{(x+1)\cdots(x+n)} e^{\frac{x}{1} + \cdots + \frac{x}{n}} \right] \\ &= \lim_{n\to\infty} \left[e^{x \lg n} \cdot \frac{1 \cdot 2 \cdots n}{(x+1)\cdots(x+n)} \right] = \lim_{n\to\infty} \frac{n^x n!}{(x+1)\cdots(x+1)}, \end{aligned}$$

in Übereinstimmung mit S. 23]. Mit dieser Identifizierung ist zugleich die Gültigkeit der *Gauss*schen Darstellung für komplexe x dargetan.

Summation der $S_{2k} = 1 - \frac{1}{2^{2k}} + \frac{1}{3^{2k}} + \cdots$ und die Bernoullischen Zahlen.

Multipliziert man das zunächst aus endlich vielen n Faktoren bestehende Produkt

$$\left(\frac{1}{x^2} - \frac{1}{1^2}\right)\left(\frac{1}{x^2} - \frac{1}{2^2}\right) \cdots \left(\frac{1}{x^2} - \frac{1}{n^2}\right)$$

IV, 32 aus, so erhält man eine Entwicklung

$$\frac{1}{x^{2n}} + a_1 \frac{1}{x^{2n-2}} + a_2 \frac{1}{x^{2n-4}} + \cdots + a_n,$$

wo die a_i die mit dem Vorzeichen $(-1)^i$ versehenen el. symm. Funktionen i–ter Dimension der Brüche $\frac{1}{1^2}, \frac{1}{2^2}, \ldots, \frac{1}{n^2}$ sind. Multiplizieren wir die beiden Entwicklungen mit x^{2n}, so wird

$$\left(1 - \frac{x^2}{1^2}\right) \cdots \left(1 - \frac{x^2}{n^2}\right) = 1 + a_1 x^2 + a_2 x^4 + \cdots + a_n x^{2n}. \tag{1}$$

Zwischen den a_i und den Potenzsummen

$$s_i = \frac{1}{1^{2i}} + \cdots + \frac{1}{n^{2i}}$$

bestehen dann die bekannten Newtonschen Formeln:

$$\begin{array}{lrcl} & 0 & = & s_1 + a_1 \\ (2) & 0 & = & s_2 + a_1 s_1 + 2a_2 \\ & 0 & = & s_3 + a_1 s_2 + a_2 s_1 + 3a_3 \\ & \multicolumn{3}{l}{\dots\dots\dots\dots\dots\dots\dots\dots} \end{array}$$

Wir machen nun mit *Euler* die kühne Annahme, daß diese Beziehungen auch noch für $n = \infty$ ihre Gültigkeit behalten. Dann geben aber die beiden Seiten von (1) die Produkt– bezw. Reihenentwicklung für $\frac{\sin \pi x}{\pi x}$. Wir erhalten also aus

$$\frac{\sin \pi x}{\pi x} = \left(1 - \frac{x^2}{1^2}\right)\left(1 - \frac{x^2}{2^2}\right) \cdots = 1 - \frac{\pi^2 x^2}{3!} + \frac{\pi^4 x^4}{5!} - \cdots ,$$

wenn wir nunmehr mit S_{2k} die unendlichen Reihen

$$S_{2k} = \frac{1}{1^{2k}} + \frac{1}{2^{2k}} + \cdots$$

bezeichnen, zu deren rekurrenter Berechnung die Formeln:

$$\begin{array}{lrcl} & 0 & = & S_2 - \frac{\pi^2}{3!} \\ (3) & 0 & = & S_4 - \frac{\pi^2}{3!} S_2 + 2\frac{\pi^4}{5!} \\ & 0 & = & S_6 - \frac{\pi^2}{3!} S_4 + \frac{\pi^4}{5!} S_2 - 3\frac{\pi^6}{7!} \\ & \multicolumn{3}{l}{\dots\dots\dots\dots\dots\dots\dots\dots} \end{array}$$

Aus ihnen folgt z. B. IV, 33

$$S_2 = \frac{\pi^2}{6}, \; S_4 = \frac{\pi^4}{90}, \; S_6 = \frac{\pi^6}{945}, \; \dots$$

Man sieht, daß allgemein S_{2k} aus π^{2k} durch Multiplikation mit einer rationalen Zahl entsteht. Die $\frac{(2k)!}{2^{2k-1}}$–fachen dieser Faktoren heißen die *Bernoullischen Zahlen* B_{2k}. (*Bernoulli* stieß 1713 bei Wahrscheinlichkeitsproblemen und bei den *Bernoullischen Polynomen* $1^m + 2^m + \cdots + n^m$ von endlicher Gliederzahl zuerst auf diese Zahlen). Dieselben sind also selbst rational definiert durch

$$S_{2k} = B_{2k} \frac{2^{2k-1}}{(2k)!} \pi^{2k}$$

oder

$$B_{2k} = \frac{(2k)!}{2^{2k-1}} \frac{S_{2k}}{\pi^{2k}}.$$

Die ersten *Bernoulli*schen Zahlen heißen $B_2 = \frac{1}{6}$, $B_4 = \frac{1}{30}$, $B_6 = \frac{1}{42}$, $B_8 = \frac{1}{30}$, $B_{10} = \frac{5}{66}$, $B_{12} = \frac{691}{2730}$, $B_{14} = \frac{7}{6}$ und wachsen dann bald ins Ungeheure. Aus den rekurrenten Formeln (3) kann man ebensowenig eine auch formal allgemeine Darstellung der S_{2k} und der damit zusammenhängenden B_{2k} gewinnen, wie das bei den Formeln (2) mit den s_i möglich ist. Für die B_{2k} kann man übrigens noch ein zweites, von Irrationalitäten freies System rekurrenter Formeln herleiten. Die oben gegebene Theorie der Funktion $x!$ gestattet nämlich ohne Schwierigkeit

IV, 34

folgende Reihe abzuleiten (s. *Serret–Scheffers*, II, S. 243 ff.):

$$\frac{1}{x}\left(\frac{1}{1-e^{-x}} - \frac{1}{x} - \frac{1}{2}\right) = \frac{B_2}{2!} - \frac{B_4}{4!}x^2 + \frac{B_6}{6!}x^3 - \cdots , \tag{5}$$

gültig für alle komplexen $|x| < 2\pi$

Multipliziert man links und rechts mit dem Produkt der Nenner der linken Seite und setzt für die Exponentialfunktion ihre Reihenentwicklung ein, so erhält man durch Koeffizientenvergleich das System:

$$\begin{aligned}
\frac{1}{2\cdot 2!} &= \frac{1}{3!} + \frac{B_2}{2!} \\
\frac{1}{2\cdot 4!} &= \frac{1}{5!} + \frac{B_2}{3!2!} - \frac{B_4}{4!} \\
\frac{1}{2\cdot 6!} &= \frac{1}{7!} + \frac{B_2}{5!2!} - \frac{B_4}{3!4!} + \frac{B_6}{6!} \\
&\ldots\ldots\ldots\ldots\ldots\ldots ,
\end{aligned} \tag{6}$$

das zur Berechnung der B_{2k} wohl geeignet ist. Endlich kann man für die Funktion (5) auch eine MacLaurinsche Entwicklung ansetzen und durch Koeffizientenvergleich auf eine etwas umständliche Art auch eine independente Darstellung der Bernoullischen Zahlen und damit der S_{2k} gewinnen (s. *Serret–Scheffers*, II, S. 257).

Es gelingt nicht, durch ähnliche Untersuchungen wie die über $\sin \pi x$ zu Summenformeln für die S_n mit *ungeradem* Index n zu gelangen. Man könnte an Betrachtungen über $\sin \pi x^2$, $\sin \pi x^{\frac{1}{2}}$ u. a. denken. Es resultieren jedoch keine Ergebnisse. Die Entwicklung von $\cos \pi x$ führt zur Summation der Partialreihen $\frac{1}{1^{2k}} + \frac{1}{3^{2k}} + \frac{1}{5^{2k}} + \cdots$. Aber diese läßt sich auch ohne Weiteres aus S_{2k} ableiten. Denn es ist:

$$2^{-2k} S_{2k} = \frac{1}{2^{2k}} + \frac{1}{4^{2k}} + \cdots ,$$

und also hat man IV, 35

$$S_{2k} - 2^{-2k} S_{2k} = \frac{1}{1^{2k}} + \frac{1}{3^{2k}} + \cdots$$

Auch die Reihe $\frac{1}{1^{2k}} - \frac{1}{2^{2k}} + \frac{1}{3^{2k}} - \cdots$ mit alternierenden Vorzeichen läßt sich so ohne weiteres gewinnen.

Die Stirlingsche Reihe.

Jacob Stirling gab 1730 eine Untersuchung über die Summation von Logarithmen heraus, deren Numeri eine arithmetische Reihe bilden. Hierin würde der auch schon von *Moivre* behandelte Spezialfall $\lg x!$ für ganzzahlige x gehören. Heute nennt man *Stirlingsche Reihe* folgende auch für nicht ganzzahlige x geltende Entwicklung:

$$\lg x! = \frac{1}{2}\lg 2\pi - x + \left(x + \frac{1}{2}\right)\lg x + \frac{B_2}{1 \cdot 2}\frac{1}{x} - \frac{B_4}{3 \cdot 4}\frac{1}{x^3} + \frac{B_6}{5 \cdot 6}\frac{1}{x^5} - \cdots + \frac{(-1)^n \vartheta B_{2n+2}}{(2n+1)(2n+2)x^{2n+1}},$$

$$\text{wo} \quad 0 < \vartheta < 1 \quad \text{ist.}$$

Die Reihe ist dadurch interessant, daß sie divergiert, gleichwohl aber bei rechtzeitigem Abbrechen zur Auswertung von $\lg x!$ sehr geeignet ist. Siehe darüber Näheres bei *Serret–Scheffers*, S. 249 ff.

k	S_{2k}
2	1,64493407
3	1,20205690
4	1,08232323
5	1,03692776
6	1,01734306
7	1,00834928
8	1,00407736
9	1,00200839
10	1,00099458
………	………
22	1,00000024

4.7 Der Hilbertsche Irreduzibilitätssatz. (26.9.1927)

Hasse gives an exposition of the proof of Hilbert's irreducibility theorem, based on his notes from the course by Schmeidler. Hasse had attended Schmeidler's course on Galois theory in Göttingen in the spring of 1919. At the end Hasse refers to recent work by Dörge (a student of Schur's) which contains substantial simplifications [Dör25], [Dör26a], [Dör26b]. *Much later Hasse had a Ph.D. student investigate arbitrary fields in which Hilbert's irreducibility theorem holds. Those fields are today called "Hilbert fields". See the thesis of W. Franz* [Fra31].

IV, 36

(Nach Kolleg *Schmeidler*, Galoissche Theorie, Göttingen Frühjahr 1919)

(Neu bearbeitet 26. IX. 27)

Satz. *Sei $F(x, y, \ldots, w; q, r, \ldots, t)$ eine ganze rationale ganzzahlige Funktion ihrer Argumente und irreduzibel in allen Variablen. Dann gibt es unendlich viele ganzzahlige Wertsysteme $q, r, \ldots, t$, durch deren Einsetzen die Funktion F in $x, y, \ldots, w$ irreduzibel bleibt.*

Beweis.

1.) Ist $g(z, t)$ ein Polynom in z und t, so definiert die Gleichung $g(z, t) = 0$ eine algebraische Funktion $z(t)$. Ist

$$g(z, t) = z^n + S_1(t)z^{n-1} + \cdots + S_n(t),$$

so ist $z(t)$ n–deutig. Seien

$$z_1(t), \ldots, z_n(t)$$

die Wurzeln der Gleichung, so haben diese n Werte unserer algebraischen Funktion im Unendlichen Entwicklungen

$$z_\lambda = \alpha_{\lambda 0}\tau^h + \alpha_{\lambda 1}\tau^{h-1} + \cdots + \alpha_{\lambda h} + \frac{\beta_{\lambda 1}}{\tau} + \frac{\beta_{\lambda 2}}{\tau^2} + \cdots ,$$

wo $\tau = t^{\frac{1}{r}}$ mit positiv–ganzzahligem r eine für alle n Zweige gleichzeitig brauchbare Uniformisierende sei (r als kleinstes Multiplum der zu den Einzelzweigen gehörigen r_λ). Ferner sei C so bestimmt, daß alle n Reihen für $|\tau| > C$, d. h. $|t| > C^r$ konvergieren. h sei genügend groß gewählt, sodaß man für alle n Reihen mit dem gleichen Anfangsexponenten h auskommt.

IV, 37

2.) Angenommen $g(z,t)$ sei für jedes ganzzahlige t_0 reduzibel. Wir wählen dann ein $\tau_0 > C$ so, daß $\tau_0^r = t_0$ ganzzahlig ausfällt. Die n Potenzreihen konvergieren dann für τ_0.

Der in $g(z,t_0)$ steckende ganzzahlige Faktor sei

$$\varphi(z) = (z - z_{i_1}) \cdots (z - z_{i_{\overline{n}}}) \qquad (1 \leqq \overline{n} \leqq n-1),$$

wobei die $z_{i_1}, \dots, z_{i_{\overline{n}}}$ gewisse der Potenzreihen aus 1.), für τ_0 gebildet, sind. Für die Auswahl dieser Wurzeln, d. h. für die Abspaltung irgendeines echten Faktors gibt es formal $\binom{n}{1} + \cdots + \binom{n}{n-1} = 2^n - 2 = a$ Möglichkeiten. Wir bezeichnen die ihnen entsprechenden Faktoren mit $\varphi_1(z), \dots, \varphi_a(z)$, und haben für diese Darstellungen

$$\varphi_k(z) = z^{\overline{n}} + \mathfrak{P}_k^{(1)}(\tau_0) z^{\overline{n}-1} + \cdots + \mathfrak{P}_k^{(\overline{n})}(\tau_0),$$

wo die Koeffizienten als elementarsymmetrische Funktionen gewisser z_λ wieder Potenzreihen in τ_0 sind.

Entsprechendes gilt, wenn wir $\sigma\tau_0$ für τ_0, also $\sigma^r t_0$ für t_0 setzen, wo $\sigma = 1, 2, 3, \dots$ Die Koeffizienten der möglichen Faktoren von $g(z, \sigma^r t_0)$ sind dann

$$\mathfrak{P}_k^{(1)}(\sigma\tau_0),\ \mathfrak{P}_k^{(2)}(\sigma\tau_0), \dots, \mathfrak{P}_k^{(\overline{n})}(\sigma\tau_0) \left\{ \begin{array}{l} k = 1, 2, \dots, a \\ \sigma = 1, 2, \dots \end{array} \right\}$$

Bei festem τ_0 ist IV, 38

$$\mathfrak{P}_k^{(\lambda)}(\sigma\tau_0) = \overline{\mathfrak{P}}_k^{(\lambda)}(\sigma)$$

eine Potenzreihe in σ. Nach unserer Annahme gibt es dann für jedes ganze positive σ einen Index k, sodaß alle $\overline{\mathfrak{P}}_k^{(\lambda)}(\sigma)$ $(\lambda = 1, \dots, \overline{n})$ ganzzahlig ausfallen.

3.) Es sei k_σ ein zu σ entsprechend 2.) gehöriger Index. Wir zeigen dann zunächst, daß es $m-1$ ganze Zahlen

$$0 < \delta_1 < \delta_2 < \cdots < \delta_{m-1}$$

gibt, sodaß

$$k_\mu, k_{\mu+\delta_1}, k_{\mu+\delta_2}, \dots, k_{\mu+\delta_{m-1}}$$

für unendlich viele μ denselben Wert k haben. Dabei ist m eine beliebige ganze positive Zahl.

Da ein k_σ nur die Werte $1, \dots, a$ haben kann, sind in einem Intervall der Länge $1 + (m-1)a$ für σ mindestens m Werte k_σ einander gleich, etwa gleich k'. Die ersten m der σ, für die dies im Intervall wirklich zutrifft, seien

$$\sigma = \mu' < \mu' + \delta_1' < \cdots < \mu' + \delta_{m-1}'$$

In einem weiteren Intervall der Länge $1+(m-1)a$ für σ sei für

$$\sigma=\mu''<\mu''+\delta_1''<\cdots<\mu''+\delta_{m-1}''$$

immer $k_\sigma=k''$. U. s. f. Die Werte $k',k'',\ldots$ liegen sämtlich in $1,\ldots,a$. Auch die Anzahl der Wertsysteme $\{\delta_1',\ldots,\delta_{m-1}'\}$, $\{\delta_1'',\ldots,\delta_{m-1}''\},\ldots$ ist beschränkt, da die δ sämtlich der Ungleichung $\delta\leqq 1+(m-1)a$ genügen. Daher ist auch die Anzahl der Kombinationen aus der Folge $k',k'',\ldots$ und der Folge $\{\delta_1',\ldots,\delta_{m-1}'\}$, IV, 39 $\{\delta_1'',\ldots,\delta_{m-1}''\},\ldots$ zu Paaren beschränkt. Es kommt also mindestens ein solches Paar unendlich oft vor. Sei k und $\{\delta_1,\ldots,\delta_{m-1}\}$ ein solches. Dann ist in der Tat für unendlich viele Zahlen μ (nämlich die den $\mu',\mu'',\ldots$ entsprechenden aus der ausgesonderten „Diagonalfolge")

$$k_\mu=k_{\mu+\delta_1}=\cdots=k_{\mu+\delta_{m-1}}=k.$$

Das bedeutet dann, daß für alle diese unendlich vielen

$$\sigma=\mu,\mu+\delta_1,\ldots,\mu+\delta_{m-1}$$

stets *ein– und dasselbe* Teilsystem der Wurzeln von $g(z,t)$ einen ganzzahligen Faktor $\varphi_k(z)$ von $g(z,\sigma^r t_0)$ liefert, nämlich mit den Koeffizienten

$$\overline{\mathfrak{P}}_k^{(1)}(\sigma),\ldots,\overline{\mathfrak{P}}_k^{(\overline{n})}(\sigma).$$

4.) Es sei nun $m-2$ nicht kleiner als der Exponent des höchsten in mindestens einer dieser Reihen vorkommenden Gliedes*), sodaß geschrieben werden kann

$$\begin{aligned}\overline{\mathfrak{P}}_k^{(\lambda)}(\sigma)&=A_{k2}^{(\lambda)}\sigma^{m-2}+\cdots+A_{km}^{(\lambda)}+B_{k1}^{(\lambda)}\frac{1}{\sigma}+B_{k2}^{(\lambda)}\frac{1}{\sigma^2}+\cdots\\&=\overline{\mathfrak{A}}_k^{(\lambda)}(\sigma)+\overline{\mathfrak{B}}_k^{(\lambda)}(\sigma)\end{aligned}$$

Wir bilden dann aus den Hauptteilen $\overline{\mathfrak{A}}_k^{(\lambda)}(\sigma)$ für $\sigma=\mu,\mu+\delta_1,\ldots,\mu+\delta_{m-1}$ die Taylor–Entwicklungen:

$$\begin{aligned}\overline{\mathfrak{A}}_k^{(\lambda)}(\mu)&=\overline{\mathfrak{A}}_k^{(\lambda)}(\mu)\\\overline{\mathfrak{A}}_k^{(\lambda)}(\mu+\delta_1)&=\overline{\mathfrak{A}}_k^{(\lambda)}(\mu)+\tfrac{\delta_1}{1!}\overline{\mathfrak{A}}_k^{(\lambda)\prime}(\mu)+\cdots+\tfrac{\delta_1^{m-2}}{(m-2)!}\overline{\mathfrak{A}}_k^{(\lambda)(m-1)}(\mu)\\&\cdots\cdots\cdots\\\overline{\mathfrak{A}}_k^{(\lambda)}(\mu+\delta_{m-1})&=\overline{\mathfrak{A}}_k^{(\lambda)}(\mu)+\tfrac{\delta_{m-1}}{1!}\overline{\mathfrak{A}}_k^{(\lambda)\prime}(\mu)+\cdots+\tfrac{\delta_{m-1}^{m-2}}{(m-2)!}\overline{\mathfrak{A}}_k^{(\lambda)(m-1)}(\mu).\end{aligned}$$

Dann existieren ganze Zahlen $u_0, \dots, u_{m-1}$, sodaß IV, 40

$$0 = u_0 \overline{\mathfrak{A}}_k^{(\lambda)}(\mu) + u_1 \overline{\mathfrak{A}}_k^{(\lambda)}(\mu + \delta_1) + \cdots + u_{m-1} \overline{\mathfrak{A}}_k^{(\lambda)}(\mu + \delta_{m-1})$$

ist *für alle ausgewählten* μ *und alle* $\lambda = 1, \dots, \overline{n}$. Dann wird also

$$\sum_{i=0}^{m-1} u_i \overline{\mathfrak{P}}_k^{(\lambda)}(\mu + \delta_i) = \sum_{i=0}^{m-1} u_i \sum_{\varrho=1}^{\infty} B_{k\varrho}^{(\lambda)} \frac{1}{(\mu + \delta_i)^\varrho}$$

eine Potenzreihe mit nur negativen Potenzen. Nun ist für hinreichend große μ,

$$\frac{1}{(\mu + \delta_i)^\varrho} = \frac{1}{\mu^\varrho} \frac{1}{\left(1 + \frac{\delta_i}{\mu}\right)^\varrho} = \frac{1}{\mu^\varrho}\left(1 + \binom{-\varrho}{1}\frac{\delta_i}{\mu} + \binom{-\varrho}{2}\frac{\delta_i^2}{\mu^2} \cdots\right)$$

(und die Koeffizienten $\binom{-\varrho}{\nu} = \frac{(-\varrho)(-\varrho-1)\cdots\left(-\varrho-(\nu-1)\right)}{1\cdot 2\cdots\nu} = (-1)^\nu\binom{\varrho+\nu-1}{\nu}$ sind ganzzahlig). Damit wird

$$\sum_{i=0}^{m-1} u_i \overline{\mathfrak{P}}_k^{(\lambda)}(\mu + \delta_i) = \sum_{\varrho=1}^{\infty}\sum_{\nu=0}^{\infty} B_{k\varrho}^{(\lambda)} (-1)^\nu \binom{\varrho + \nu - 1}{\nu} \frac{1}{\mu^{\varrho+\nu}} \sum_{i=0}^{m-1} u_i \delta_i^\nu .$$

Nach Bestimmung der u_i ist nun

$$\sum_{i=0}^{m-1} u_i \delta_i^\nu = 0 \quad \text{für} \quad \nu = 0, 1, \dots, m-2$$

Weil aber die Determinante $|\delta_i^\nu| \neq 0$ ist $\begin{pmatrix} i = 0, \dots, m-1 \\ \nu = 0, \dots, m-1 \end{pmatrix}$, als Differenzenprodukt von $0 = \delta_0 < \delta_1 < \cdots < \delta_{m-1}$, so ist sicher

$$\sum_{i=0}^{m-1} u_i \delta_i^{m-1} \neq 0.$$

Ist ferner als erstes $B_{k\varrho_k^{(\lambda)}}^{(\lambda)} \neq 0$, so haben wir

$$\overline{P}_k^{(\lambda)}(\mu) = \sum_{i=0}^{m-1} u_i \overline{\mathfrak{P}}_k^{(\lambda)}(\mu + \delta_i) = \sum_{\varrho=\varrho_k^{(\lambda)}}^{\infty} \sum_{\nu=m-1}^{\infty} \frac{B_{k\varrho}^{(\lambda)}\binom{\varrho+\nu-1}{\nu}}{\mu^{\varrho+\nu}} \sum_{i=0}^{m-1} u_i \delta_i^\nu$$

IV, 41 Wir bestimmen den ersten Koeffizienten dieser nach negativen Potenzen von μ fortschreitenden Reihe, also den von $\frac{1}{\mu^{\varrho_k^{(\lambda)}+m-1}}$. Dieser ist

$$b_{k0}^{(\lambda)} = B_{k\varrho_k^{(\lambda)}}^{(\lambda)} \binom{\varrho_k^{(\lambda)} + m - 1}{m-1} \sum_{i=0}^{m-1} u_i \delta_i^{m-1} \neq 0.$$

Es wird also

$$\overline{P}_k^{(\lambda)}(\mu) = \frac{b_{k0}^{(\lambda)}}{\mu^{\varrho_k^{(\lambda)}+m-1}} + \frac{b_{k1}^{(\lambda)}}{\mu^{\varrho_k^{(\lambda)}+m}} + \cdots$$

Nun ist auch $\overline{P}_k^{(\lambda)}(\mu)$, wegen der Ganzzahligkeit der u_i für unendlich viele μ eine ganze Zahl. Weil nun $\lim\limits_{\mu\to\infty} \overline{P}_k^{(\lambda)}(\mu) = 0$ ist, wird diese ganze Zahl Null sein, wenn μ hinreichend groß ist. Andererseits ist

$$\overline{P}_k^{(\lambda)}(\mu)\mu^{\varrho_k^{(\lambda)}+m-1} = b_{k0}^{(\lambda)} + \frac{b_{k1}^{(\lambda)}}{\mu} + \cdots,$$

und der Rest vom zweiten Glied rechts ist für hinreichend großes μ beliebig klein. Für hinreichend große μ ist aber nach dem eben Gezeigten die linke Seite Null, sodaß ein Widerspruch mit $b_{k0}^{(\lambda)} \neq 0$ herauskommt. Daher kann kein erster Koeffizient $B_{k\varrho_k^{(\lambda)}}^{(\lambda)} \neq 0$ existieren. Es ist daher notwendig $\overline{\mathfrak{B}}_k^{(\lambda)}(\sigma) \equiv 0$, d. h.

$$\begin{aligned} \overline{\mathfrak{P}}_k^{(\lambda)}(\sigma) &= \overline{\mathfrak{A}}_k^{(\lambda)}(\sigma) \quad \text{ganz rational in } \sigma. \\ &= A_{k2}^{(\lambda)}\sigma^{m-2} + \cdots + A_{km}^{(\lambda)}. \end{aligned}$$

Diese Polynome in σ sind nun für unendlich viele σ ganze Zahlen. Daher sind die Koeffizienten $A_{ki}^{(\lambda)}$rational (Auflösung von $m-1$ Gleichungen mit verschiedenen IV, 42 σ nach den Koeffizienten).

5.) Ferner ist bewiesen, daß *identisch in* σ

$$\overline{\mathfrak{P}}_k^{(\lambda)}(\sigma) = A_{k2}^{(\lambda)}\sigma^{m-2} + \cdots + A_{km}^{(\lambda)}$$

gilt, weil ja bewiesen ist, daß alle folgenden Koeffizienten verschwinden. Setzen wir also $\sigma\tau_0 = \tau$, so gilt nach Konstruktion

$$\overline{\mathfrak{P}}_k^{(\lambda)}\left(\frac{\tau}{\tau_0}\right) = \mathfrak{P}_k^{(\lambda)}(\tau) = A_{k2}^{(\lambda)}\left(\frac{\tau}{\tau_0}\right)^{m-2} + \cdots + A_{km}^{(\lambda)}$$

*) m muß korrekterweise unabhängig von der Auswahl des unter Verwendung von m definierten Potenzreihsystems definiert werden. Ersichtlich genügt $m - r \geqq (n-1)h$, wo h die Bedeutung von S. 36]/37] hat.

identisch in τ. Folglich ist der dem Index k entsprechende Faktor von $g(z,t)$ IV, 43 ein Polynom in z, dessen Koeffizienten *identisch in* $\tau = t^{\frac{1}{r}}$ ganz–rational sind mit rationalen Zahlkoeffizienten. Ähnlich wie oben können wir nun zwei verschiedene $\tau_0, \hat{\tau}_0 > C$ finden, sodaß für sie der im vorhergehenden resultierende „Zerlegungsindex“ k derselbe ist. Denn für k stehen nur endlich viele Werte $1, \ldots, a$ zur Verfügung. Überdies können $\tau_0, \hat{\tau}_0$ auch noch so gewählt werden, daß $\tau_0^r = t_0, \hat{\tau}_0^r = \hat{t}_0$ Primzahlen werden. Es gilt dann *identisch in* τ

$$\mathfrak{P}_k^{(\lambda)}(\tau) = \overline{\mathfrak{P}}_k^{(\lambda)}\left(\frac{\tau}{\tau_0}\right) = \overline{\mathfrak{P}}_k^{(\lambda)}\left(\frac{\tau}{\hat{\tau}_0}\right),$$

wobei

$$\overline{\mathfrak{P}}_k^{(\lambda)}\left(\frac{\tau}{\hat{\tau}_0}\right) = \hat{A}_{k2}^{(\lambda)}\left(\frac{\tau}{\hat{\tau}_0}\right)^{m-2} + \cdots + \hat{A}_{km}^{(\lambda)}$$

mit ebenfalls rationalen Zahlkoeffizienten ist. Somit ist dann

$$\hat{A}_{k\varrho}^{(\lambda)}\frac{1}{\hat{\tau}_0^{m-\varrho}} = A_{k\varrho}^{(\lambda)}\frac{1}{\tau_0^{m-\varrho}} \qquad (\varrho = 2, \ldots, m),$$

oder

$$\frac{\hat{A}_{k\varrho}^{(\lambda)}}{A_{k\varrho}^{(\lambda)}} = \frac{\hat{\tau}_0^{m-\varrho}}{\tau_0^{m-\varrho}} = \frac{\hat{t}_0^{\frac{m-\varrho}{r}}}{t_0^{\frac{m-\varrho}{r}}}.$$

Geht nun r nicht in $m - \varrho$ auf, so ist nach Wahl von $t_0, \hat{t}_0$ die rechte Seite eine irrationale Zahl. Die linke Seite dagegen ist (sofern nicht Zähler und Nenner verschieden und die Betrachtung so nicht durchführbar ist) rational. Daher müssen alle Koeffizienten $A_{k\varrho}^{(\lambda)}, \hat{A}_{k\varrho}^{(\lambda)}$, für die r nicht in $m - \varrho$ aufgeht, verschwinden. Dann ist aber ersichtlich $\mathfrak{P}_k^{(\lambda)}(\tau)$ identisch rational in $t = \tau^r$ mit rationalen Koeffizienten, und somit auch der Faktor von $g(z,t)$, der dem Index k entspricht, von dieser Art, also $g(z,t)$ reduzibel.

6.) Damit ist zunächst festgestellt: Besitzt ein ganzzahliges Polynom $g(z,t) =$ IV, 44 $z^n + S_1(t)z^{n-1} + \cdots + S_n(t)$ für jedes ganze t_0 einen echten ganzzahligen Teiler in z, so besitzt $g(z,t)$ einen echten rationalzahligen Teiler in z, t. (Dieser ist dann übrigens nach dem verallgemeinerten Gaussschen Satz sogar ganzzahlig). Hat $g(z,t)$ nicht den höchsten Koeffizienten 1 in z, so hat jedenfalls

$\big(S_0(t)\big)^{n-1} g(z,t) = \overline{g}\big(S_0(t)z,t\big)$ diese Eigenschaft in $S_0(t)z$, wenn $S_0(t)$ der höchste Koeffizient in z ist. Ist nun $g(z,t)$ für jedes ganze t_0 reduzibel in z, so ist sicher auch $\overline{g}\big(S_0(t)z,t\big)$ für jedes ganze t_0 reduzibel in $S_0(t)z$, weil ja für $t = t_0$ z und $S_0(t)z$ nur um eine ganze Zahl als Faktor unterschieden sind. Also ist $\overline{g}\big(S_0(t)z,t\big)$ nach unserem Beweis reduzibel in $S_0(t)z, t$. Es besteht dann eine Zerlegung

$$\overline{g}\big(S_0(t)z,t\big) = S_0(t)^{n-1} g(z,t) = \varphi_1\big(S_0(t)z,t\big) \cdot \varphi_2\big(S_0(t)z,t\big).$$

Hier ist die linke Seite teilbar durch $S_0(t)^{n-1}$. Folglich kann jeder Primfaktor von $S_0(t)^{n-1}$ einzeln aus einem der beiden Faktoren links weggehoben werden, und zwar sowohl die Zahl– als auch die Funktionsfaktoren (eindeutige Primzerlegung im Integritätsbereich der ganzzahligen Polynome in z,t). Daher ist dann auch $g(z,t)$ selbst reduzibel in z,t.

Schließlich zeigt unser Beweis, daß es genügt, die Reduzibilität für *alle hinreichend großen* ganzen t_0 vorauszusetzen. Ist also $g(z,t)$ irreduzibel in z,t, so existiert über jeder Grenze T noch ein ganzes t_0, für das $g(z,t_0)$ irreduzibel in z ist, somit *unendlich viele* t_0, wie behauptet.

Die Ausdehnung des Beweises auf Polynome in mehr als 2 Veränderlichen läßt sich jedenfalls nicht ohne weiteres durch vollständige Induktion führen. Man muß vielmehr den den bisherigen Beweis von Grund aus verallgemeinern.

(Siehe die Arbeiten von *Dörge*).

4.8 Die Dichte der Primzahlen p, für die a primitive Wurzel ist. (27.9.1927)

This is the first document which contains the celebrated Artin conjecture on primitive roots. Artin had visited Hasse on September 13, 1927. Originally they wished to discuss the implications of Artin's reciprocity law which he had succeeded to prove just two months ago. But apparently they talked also about other things, as this and the following entries show. See in particular the entry of September 28, 1927 where Hasse notes some more ideas towards the problem.] In these entries Hasse mentions the three "Axioms of Tornier". This refers to their joint paper [HT28] *where they stated* 3 *axioms which guarantee the existence of density and a limit formula for its value. That paper had been submitted on June 15, 1927, hence only a few weeks before Artin's visit. It appears plausible that Hasse had told Artin about this new paper, and Artin had provided on the spot his problem on primitive roots as a test whether the Hasse-Tornier axioms could be used successfully to solve the problem. See also the entry of September 28, 1927.] – Note that already here there appears the error in the computation of the expected density. The point is that the fields K_q (in Hasse's notation) are not necessarily independent. It was many years later only that Artin discovered this error following a letter of Emma Lehmer who had informed him that the numerical evidence did not comply with Artin's expected density, so that Artin had to modify it. See* [Ste03].

IV, 45

(Nach mündlicher Mitteilung von *Artin* 13. IX. 27)

(27. IX. 27)

Es sei $a > 1$ eine positive ganze Zahl, die nicht Potenz einer kleineren positiven ganzen Zahl ist. Damit a primitive Wurzel für eine Primzahl p ist, die prim zu $2, 3, a$ vorausgesetzt wird, ist notwendig und hinreichend, daß die Kongruenz

$$x^q \equiv a \mod. p$$

für keine Primzahl $q|p-1$ eine Lösung besitzt. Da diese Kongruenz für $q|p-1$ mit einer Lösung stets q verschiedene Lösungen besitzt, und für die $q \nmid p-1$ und $q \neq p$ stets eine aber auch nur eine Lösung besitzt, kann man das Kriterium auch so aussprechen:

Eine zu $2, 3, a$ *prime Primzahl* p *hat* a *dann und nur dann zur primitiven Wurzel, wenn die Kongruenz*

$$x^q \equiv a \ \text{mod.}\, p$$

für keine Primzahl $q \neq p$ q *verschiedene Lösungen besitzt.*

Dann und nur dann, wenn jene Kongruenz für ein zu $2, 3, a$ primes $p \neq q$ q verschiedene Lösungen besitzt, zerfällt p in $R(\sqrt[q]{a})$ in verschiedene Primideale 1. Grades, kurz: p *zerfällt voll in* $R(\sqrt[q]{a})$. (Die Diskriminante von $R(\sqrt[q]{a})$ hat höchstens q und Primteiler von a zu Teilern, und kein davon verschiedenes p ist Teiler der Diskriminante von $x^q - a$). Dann und nur dann, wenn das letztere für ein zu $2, 3, a$ primes $p \neq q$ der Fall ist, zerfällt ferner p voll im zugehörigen Galoisschen Körper $R(\zeta_q, \sqrt[q]{a})$, wo ζ_q eine primitive q–te Einheitswurzel ist. Da IV, 46 nun q selbst sicher in der Diskriminante von $R(\zeta_q, \sqrt[q]{a})$ aufgeht, wenn $q \neq 2$ ist, und da $p = q$ wegen p prim zu 2 nur für $q \neq 2$ vorkommt, kann die Einschränkung $p \neq q$ fallen gelassen werden, wenn man das Kriterium in $R(\zeta_q, \sqrt[q]{a})$ formuliert:

Eine zu $2, 3, a$ *prime Primzahl* p *hat* a *dann und nur dann zur primitiven Wurzel, wenn* p *in keinem Körper* $K_q = R(\zeta_q, \sqrt[q]{a})$ *voll zerfällt.*

Es seien nun $P_q(N), P_{q_1 \dots q_n}(N)$ die Anzahlen der Primzahlen $p \leqq N$, die in K_q bezw. in $K_{q_1}, \dots, K_{q_n}$, d. h. im Kompositum $K_{q_1 \dots q_n} = (K_{q_1}, \dots, K_{q_n})$ voll zerfallen. Da K_q den Grad $q(q-1)$ und $K_{q_1 \dots q_n}$ wegen der Unabhängigkeit der K_{q_i} den Grad $\prod_{i=1}^n q_i(q_i - 1)$ hat, so gilt bekanntlich

$$P_q(N) \sim \frac{1}{q(q-1)} \cdot \operatorname{Li} N,$$
$$P_{q_1 \dots q_n}(N) \sim \prod_{i=1}^n \frac{1}{q_i(q_i - 1)} \cdot \operatorname{Li} N.$$

Dividiert man das durch die asymptotische Formel

$$P(N) \sim \operatorname{Li} N$$

für die Anzahl *aller* Primzahlen $p \leqq N$, so erhält man:

$$\frac{P_q(N)}{P(N)} \sim \frac{1}{q(q-1)}, \quad \frac{P_{q_1 \dots q_n}(N)}{P(N)} \sim \prod_{i=1}^n \frac{1}{q_i(q_i - 1)}.$$

Hiermit ist für die in den $P_q(N), P_{q_1\ldots q_n}(N)$ gezählten Ereignisse E_q, nämlich das volle Zerfallen von p in K_q, und die Folge aller Primzahlen p (prim zu $2, 3, a$) IV, 47 als Grundfolge das erste *Tornier*sche Postulat (multiplikatives Verhalten der „Primdichten") festgestellt. Auch das zweite *Tornier*sche Postulat, daß jedem Element p nur endlich viele E_q zukommen, ist erfüllt, weil ja $q|p-1$ sein muß, wenn E_q p zukommt. Fraglich ist nur das dritte *Tornier*sche Postulat:

$$\frac{P_q(N)}{P(N)} < \frac{c_q}{q(q-1)}$$

für alle $N \geqq N_0$ und alle q, wo die c_q eine Zahlfolge, sodaß $\sum\limits_q \frac{c_q}{q(q-1)}$ konvergiert.

Dessen Bestätigung würde die Untersuchung der Abhängigkeit der Restabschätzung in der obigen asymptotischen Formel für $P_q(N)$ von q erfordern.

Setzt man dieses dritte Postulat als bewiesen voraus, so folgt nach dem *Tornier*schen Schema für die Dichte der Primzahlen p, denen keine Eigenschaft E_q zukommt, und das sind eben gerade diejenigen p (prim zu $2, 3, a$), für die a primitive Wurzel ist, die Relation

$$\frac{\overline{P}(N)}{P(N)} \sim \prod_q \left(1 - \frac{1}{q(q-1)}\right).$$

Dabei bezeichnet also $\overline{P}(N)$ die Anzahlen der Primzahlen $p \leqq N$, für die a primitive Wurzel ist, $P(N)$ die Anzahl aller Primzahlen $p \leqq N$ (die Einschränkung prim zu $2, 3, a$ ist jetzt natürlich entbehrlich).

Man findet übrigens

$$\frac{1}{4} < \prod_q \left(1 - \frac{1}{q(q-1)}\right) < \frac{5}{12}.$$

IV, 48

Von der Einschränkung, daß a nicht Potenz einer kleineren Zahl sei, ist nur insofern Gebrauch gemacht worden, als von der Zerlegung von $x^q - a$ mod. p in verschiedene Linearfaktoren auf das volle Zerfallen von p in $K_q = R(\zeta_q, \sqrt[q]{a})$ geschlossen wurde. Ist nun a eine q'–te Potenz, so zerfällt ein zu $2, 3, a$ primes p dann und nur dann voll in $K'_{q'} = R(\zeta_{q'})$, wenn $q'|p-1$ ist, und dann und nur dann hat $x^{q'} \equiv a$ mod. p q' verschiedene Lösungen. Anstelle von K_q tritt also für solche q' einfach der Körper $K'_{q'}$ vom Grade $q'-1$. Daher führt dieselbe Überlegung zu der allgemeinen Formel

$$\frac{\overline{P}(N)}{P(N)} \sim \prod_q{}' \left(1 - \frac{1}{q(q-1)}\right) \cdot \prod_{q'} \left(1 - \frac{1}{q'-1}\right),$$

wo q im ersten Produkt alle unendlich vielen Primzahlen durchläuft, für die a keine q–te Potenz ist, während q' im zweiten Produkt alle endlich vielen Primzahlen durchläuft, für die a eine q'–te Potenz ist.

(Siehe auch S. 58])

4.9 Beweis des Hauptsatzes der Idealtheorie. (27.9.1927)

This is the simplified version of Emmy Noether's exposition which Artin had presented in his lecture in Hamburg. Artin on his visit to Hasse had told him the essentials of the proof and Hasse now writes down the exposition. We note that this proof has later been included in van der Waerden's book "Moderne Algebra". For, van der Waerden had attended Artin's lecture.

IV, 49

(Nach mündlicher Mitteilung von *Artin*, 13. IX. 27)

(27. IX. 27).

Es sei $\mathfrak{J}$ ein Integritätsbereich, in dem die *E. Noether*schen Axiome erfüllt sind:

(I.) Doppelkettensatz: *Jede Teiler–Vielfachenkette*

$$\cdots|\mathfrak{a}_{-2}|\mathfrak{a}_{-1}|\mathfrak{a}_0|\mathfrak{a}_1|\mathfrak{a}_2|\cdots|\mathfrak{a}$$

von Idealen aus $\mathfrak{J}$, die sämtlich Teiler eines festen Ideals $\mathfrak{a} \neq 0$ aus $\mathfrak{J}$ sind, bricht nach oben und unten dadurch ab, daß alle Ideale der Kette von einer Stelle an gleich sind, und zwar tritt dies nach endlich vielen Gliedern ein.

(II.) Ganz–algebraische Abgeschlossenheit: *Genügt ein Element μ des Quotientenkörpers K von $\mathfrak{J}$ einer Gleichung*

$$\mu^n + \alpha_1\mu^{n-1} + \cdots + \alpha_n = 0$$

mit höchstem Koeffizienten 1 und Koeffizienten $\alpha_1, \ldots, \alpha_n$ aus $\mathfrak{J}$, so gehört μ zu $\mathfrak{J}$.

Ich nenne im folgenden die Elemente aus $\mathfrak{J}$ *ganz*, die nicht zu $\mathfrak{J}$ gehörigen aus K *gebrochen.*

Hilfssatz 1. *Jedes Ideal $\mathfrak{a}$ aus $\mathfrak{J}$ besitzt eine endliche Basis*

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r).$$

Beweis: Es sei α_1 ein Element aus $\mathfrak{a}$. Entweder ist dann $\mathfrak{a} = (\alpha_1)$, oder es ist $\mathfrak{a}_1 = (\alpha_1)$ ein echtes Vielfaches von $\mathfrak{a}$, und es gibt noch ein nicht zu $\mathfrak{a}_1$ gehöriges

Element α_2 in $\mathfrak{a}$. Dann ist $\mathfrak{a}_2 = (\alpha_1, \alpha_2)$ echter Teiler von $\mathfrak{a}_1$. Entweder ist jetzt
IV, 50 $\mathfrak{a} = \mathfrak{a}_2$, oder $\mathfrak{a}_2$ ist echtes Vielfaches von $\mathfrak{a}_1$ und es gibt noch ein nicht zu $\mathfrak{a}_2$ gehöriges Element α_3 in $\mathfrak{a}$. Dieses Verfahren muß nach endlich vielen Schritten mit $\mathfrak{a} = \mathfrak{a}_r = (\alpha_1, \dots, \alpha_r)$ schließen, da sonst in

$$\mathfrak{a} | \cdots | \mathfrak{a}_0 | \mathfrak{a}_1$$

eine unendliche Kette echter Teiler (die überdies sämtlich echte Vielfache von $\mathfrak{a}$ sind) resultierte, entgegen Axiom (I.).

Hilfssatz 2. *Ein Ideal $\mathfrak{p}$ aus $\mathfrak{I}$ ist dann und nur dann Primideal im E. Noetherschen Sinne, d. h. aus $\mathfrak{p}|\alpha\beta$ folgt $\mathfrak{p}|\alpha$ oder $\mathfrak{p}|\beta$, wenn es Primideal im gewöhnlichen Sinne ist, d. h. keinen vom Einheitsideal $\mathfrak{o}$ und von $\mathfrak{p}$ verschiedenen Teiler besitzt.*

Beweis: a.) Es sei $\mathfrak{p}$ Primideal im gewöhnlichen Sinne. Ist dann $\mathfrak{p}|\alpha\beta$, aber $\mathfrak{p} \nmid \alpha$, so ist $(\mathfrak{p}, \alpha)$ echter Teiler von $\mathfrak{p}$, also $(\mathfrak{p}, \alpha) = \mathfrak{o}$, $(\mathfrak{p}\beta, \alpha\beta) = \beta$. Da aber $\mathfrak{p}|\mathfrak{p}\beta$ und $\mathfrak{p}|\alpha\beta$, so folgt hieraus auch $\mathfrak{p}|\beta$.
IV, 51 b.) Es sei $\mathfrak{p}$ Primideal im *E. Noether*schen Sinne. Ist dann $\mathfrak{a}$ ein echter Teiler von $\mathfrak{p}$, so gibt es in $\mathfrak{a}$ ein nicht zu $\mathfrak{p}$ gehöriges Element α. Die Vielfachenkette

$$(\alpha, \mathfrak{p}) | (\alpha^2, \mathfrak{p}) | \cdots | \mathfrak{p}$$

von Teilern von $\mathfrak{p}$ bricht dann nach endlich vielen Schritten ab:

$$(\alpha^r, \mathfrak{p}) = (\alpha^{r+1}, \mathfrak{p}).$$

Dann besteht eine Gleichung

$$\alpha^r = \gamma\alpha^{r+1} + \pi\,, \quad \text{d. h.} \quad \mathfrak{p}|\alpha^r(\gamma\alpha - 1)$$

mit ganzem γ und π aus $\mathfrak{p}$. Da aber $\mathfrak{p} \nmid \alpha$ ist, folgt $\mathfrak{p}|\gamma\alpha - 1$, also erst recht $\mathfrak{a}|\gamma\alpha - 1$ und wegen $\mathfrak{a}|\alpha$ somit auch $\mathfrak{a}|1$, d. h. $\mathfrak{a} = \mathfrak{o}$.

Hilfssatz 3. *Ist $\mathfrak{p}$ ein Primideal aus $\mathfrak{I}$, so gibt es im Ideal $\mathfrak{p}^{-1}$, d. h. in der Gesamtheit aller μ aus K, für die $\mathfrak{p}|\alpha$ ganz ist, ein gebrochenes μ.*

Beweis: Wir stellen zunächst folgende Bemerkung vorweg: Ist ein Ideal $\mathfrak{c}$ kein Primideal, so gibt es zwei echte Teiler $\mathfrak{a}, \mathfrak{b}$ von $\mathfrak{c}$, sodaß $\mathfrak{c}|\mathfrak{a}\mathfrak{b}$. Zunächst gibt es dann nämlich Elemente α, β, sodaß $\mathfrak{c}|\alpha\beta$ aber $\mathfrak{c} \nmid \alpha$, $\mathfrak{c} \nmid \beta$. Dann leisten aber $\mathfrak{a} = (\alpha, \mathfrak{c})$, $\mathfrak{b} = (\beta, \mathfrak{c})$ das Verlangte*).

*) Hier wird Teil b.) von Hilfssatz 2 angewandt, wenn man Primideal im gewöhnlichen Sinne versteht!

Sei nun $\pi \neq 0$ ein Element aus $\mathfrak{p}$. Entweder ist (π) Primideal. Oder es gibt zwei echte Teiler $\mathfrak{a}, \mathfrak{b}$ von (π), sodaß $\pi | \mathfrak{ab}$. Entweder sind ferner $\mathfrak{a}, \mathfrak{b}$ Primideale, oder man kann mit ihnen verfahren, wie eben mit (π). Dies Verfahren muß nach Axiom (I.) nach endlich vielen Schritten abbrechen, sodaß also Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ resultieren, für die $\pi | \mathfrak{p}_1 \dots \mathfrak{p}_r$ ist.

Insbesondere ist dann auch $\mathfrak{p} | \mathfrak{p}_1 \dots \mathfrak{p}_r$. Also ist $\mathfrak{p}$ Teiler eines $\mathfrak{p}_i$ und nach Hilfssatz 2 dann $\mathfrak{p} = \mathfrak{p}_i$. Hier wird benutzt, daß aus der *E. Noether*schen Primidealdefinition auch die Eigenschaft folgt, daß aus $\mathfrak{p} | \mathfrak{ab}$ folgt $\mathfrak{p} | \mathfrak{a}$ oder $\mathfrak{p} | \mathfrak{b}$. Wäre nämlich $\mathfrak{p} \nmid \mathfrak{a}$ und $\mathfrak{p} \nmid \mathfrak{b}$, so gäbe es α in $\mathfrak{a}$, β in $\mathfrak{b}$, sodaß $\mathfrak{p} \nmid \alpha$ und $\mathfrak{p} \nmid \beta$, also $\mathfrak{p} \nmid \alpha\beta$ und somit auch $\mathfrak{p} \nmid \mathfrak{ab}$ wäre. IV, 52

Wir wählen nun eine Primidealfolge $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ obiger Art mit möglichst kleinem r. Sei dabei etwa $\mathfrak{p}_1 = \mathfrak{p}$. Dann ist $\pi \nmid \mathfrak{p}_2 \dots \mathfrak{p}_r$. Ist demgemäß α Element aus $\mathfrak{p}_2 \dots \mathfrak{p}_r$, sodaß $\pi \nmid \alpha$ ist, so ist $\mu = \frac{\alpha}{\pi}$ gebrochen und $\mu\mathfrak{p} = \mu\mathfrak{p}_1 = \alpha\frac{\mathfrak{p}_1 \cdots \mathfrak{p}_r}{\pi}$ ganz, weil $\pi | \mathfrak{p}_1 \dots \mathfrak{p}_r$.

Satz 1. *Für jedes Primideal* $\mathfrak{p}$ *aus* $\mathfrak{J}$ *gilt* $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

Beweis: Nach Definition von $\mathfrak{p}^{-1}$ ist $\mathfrak{p}\mathfrak{p}^{-1}$ ganz. Da ferner 1 zu $\mathfrak{p}^{-1}$ gehört, ist $\mathfrak{p}\mathfrak{p}^{-1} | \mathfrak{p}$. Also ist $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$ oder $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ nach Hilfssatz 2.

Wäre nun $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$, so sei $\mathfrak{p} = (\pi_1, \dots, \pi_r)$ gemäß Hilfssatz 1, und μ gebrochen aus $\mathfrak{p}^{-1}$ gemäß Hilfssatz 3. Da dann die $\mu\pi_i$ zu $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ gehören, folgte

$$\mu\pi_i = \sum_{i=1}^{r} \alpha_{ij}\pi_j \quad \text{mit ganzen} \quad \alpha_{ij}.$$

Daraus ergäbe sich eine algebraische Gleichung in $\mathfrak{J}$ mit höchstem Koeffizienten 1 für das gebrochene μ, im Widerspruch zu Axiom (II.).

Satz 2. *Für jedes Primideal* $\mathfrak{p}$ *aus* $\mathfrak{J}$ *sind die Potenzen* $\mathfrak{p}^0 = \mathfrak{o}, \mathfrak{p}, \mathfrak{p}^2, \dots$ *alle verschieden.*

Beweis: Wäre $\mathfrak{p}^m = \mathfrak{p}^n$ mit $m > n \geqq 0$, so folgte nach Satz 1 $\mathfrak{p}^{m-n} = \mathfrak{o}$, also $\mathfrak{p} = \mathfrak{o}$.

Satz 3. *Jedes Ideal* $\mathfrak{a} \neq 0, \mathfrak{o}$ *aus* $\mathfrak{J}$ *besitzt eine Zerlegung* $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$ *in Primideale aus* $\mathfrak{J}$.

Beweis: Nach Axiom (I.) und Hilfssatz 2 existiert ein Primideal $\mathfrak{p}_1 | \mathfrak{a}$. Man setze $\mathfrak{a}\mathfrak{p}_1^{-1} = \mathfrak{a}_1$. Dann ist $\mathfrak{a} = \mathfrak{a}_1\mathfrak{p}_1$ nach Satz 1. Nach Definition von $\mathfrak{p}_1^{-1}$ und weil $\mathfrak{p}_1 | \mathfrak{a}$ ist $\mathfrak{a}_1$ ganz. Ferner ist $\mathfrak{a}_1 | \mathfrak{a}$, weil 1 in $\mathfrak{p}_1^{-1}$ liegt. Schließlich ist $\mathfrak{a}_1 \neq \mathfrak{a}$. Wäre nämlich $\mathfrak{a}_1 = \mathfrak{a}$, also $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_1$, so folgte $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_1^r$, d. h. $\mathfrak{p}_1^r | \mathfrak{a}$ für jedes $r \geqq 1$. Es IV, 53

wäre dann

$$\mathfrak{p}_1 | \mathfrak{p}_1^2 | \mathfrak{p}_1^3 | \cdots | \mathfrak{a}$$

eine unendliche Vielfachenkette von Teilern von $\mathfrak{a}$, die nach Satz 2 aus lauter verschiedenen Idealen besteht, entgegen Axiom (I.). Folglich ist $\mathfrak{a}_1$ echter Teiler von $\mathfrak{a}$. Auf $\mathfrak{a}_1$ wende man dieselbe Schlußweise an: $\mathfrak{a}_1 = \mathfrak{a}_2\mathfrak{p}_2, \dots$ Dies Verfahren bricht nur ab, wenn einmal $\mathfrak{a}_r = \mathfrak{o}$ wird, und muß nach Axiom (I.) wirklich abbrechen. Also resultiert $\mathfrak{a} = \mathfrak{p}_1 \dots \mathfrak{p}_r$.

Satz 4. *Die in Satz 3 genannte Zerlegung ist eindeutig.*

Beweis: Aus

$$\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{q}_1 \dots \mathfrak{q}_s$$

folgt $\mathfrak{p}_1 | \mathfrak{q}_1 \dots \mathfrak{q}_s$, also etwa $\mathfrak{p}_1 | \mathfrak{q}_1$, $\mathfrak{p}_1 = \mathfrak{q}_1$, und dann nach Satz 1

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s.$$

So fortfahrend ergibt sich die Behauptung.

IV, 54

Satz 6. *In einem Integritätsbereich $\mathfrak{J}$ gelte Hilfssatz 2, und die Sätze 3,4. Dann gelten die Axiome* (I.) *und* (II.) *in $\mathfrak{J}$.*

Beweis: a.) Aus $\mathfrak{a} \neq 0$ und $\mathfrak{b}|\mathfrak{a}$ folgt $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Ist nämlich $\mathfrak{a} = \mathfrak{p}_1^{\mu_1} \dots \mathfrak{p}_r^{\mu_r}$, $\mathfrak{b} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}$ und $\nu_1 > 0$, so gilt $\mathfrak{p}_1^{\nu_1} | \mathfrak{p}_1^{\mu_1} \mathfrak{a}_1$, wo $\mathfrak{a}_1 = \mathfrak{p}_2^{\mu_2} \dots \mathfrak{p}_r^{\mu_r}$ den Faktor $\mathfrak{p}_1$ nicht mehr enthält.
Nach Hilfssatz 2 ist nun $(\mathfrak{p}_1, \mathfrak{p}_2) = \mathfrak{o}, \dots, (\mathfrak{p}_1, \mathrm{p}_r) = \mathfrak{o}$. Folglich auch $(\mathfrak{p}_1, \mathfrak{a}_1) = \mathfrak{o}$. (Aus $(\mathfrak{a}, \mathfrak{b}_1) = \mathfrak{o}$ und $(\mathfrak{a}, \mathfrak{b}_2) = \mathfrak{o}$ folgt $(\mathfrak{a}, \mathfrak{b}_1\mathfrak{b}_2) = \mathfrak{o}$ elementar). Daher ebenso $(\mathfrak{p}_1^{\nu_1}, \mathfrak{a}_1) = \mathfrak{o}$, und daraus $(\mathfrak{p}_1^{\nu_1}, \mathfrak{p}_1^{\mu_1}\mathfrak{a}_1) = \mathfrak{p}_1^{\mathrm{Min}(\mu_1,\nu_1)}$. Denn zufolge der eindeutigen Bestimmtheit der Exponenten ist $\mathfrak{p}_1^n$ echter Teiler von $\mathfrak{p}_1^m$, wenn $n < m$, also $(\mathfrak{p}_1^{\nu_1}, \mathfrak{p}_1^{\mu_1}) = \mathfrak{p}_1^{\mathrm{Min}(\mu_1,\nu_1)}$. $\big($Aus $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ folgt elementar $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = (\mathfrak{a}, \mathfrak{c})\big)$. Daher folgt $\mathfrak{p}_1^{\nu_1} \mid \mathfrak{p}_1^{\mathrm{Min}(\mu_1,\nu_1)}$, d. h. $\nu_1 \leqq \mathrm{Min}(\mu_1, \nu_1)$, also $\nu_1 \leqq \mu_1$. Das ergibt, auf die $\mathfrak{p}_2, \dots, \mathfrak{p}_r$ ausgedehnt, in der Tat $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Daraus entnimmt man zufolge Sätzen 3,4 ohne weiteres Axiom (I.).

b.) Sei μ gebrochen, genüge aber einer algebraischen Gleichung in $\mathfrak{J}$ mit höchstem Koeffizienten 1. Dann

IV, 55

betrachten wir das Ideal $\mathfrak{m} = (1, \mu, \mu^2, \dots)$. Dieses ist gebrochen. Es besitzt aber eine endliche Basis $1, \mu, \dots, \mu^{r-1}$, wenn r der Grad der Gleichung für μ. Es ist also demgemäß, wenn $\mu = \frac{\beta}{\gamma}$ mit ganzen β, γ ist $\mathfrak{m}\gamma^{r-1} = \mathfrak{a}$ ein ganzes Ideal in $\mathfrak{J}$, d. h. $\mathfrak{m} = \frac{\mathfrak{a}}{\gamma^{r-1}}$. Nun ist ersichtlich $\mathfrak{m}^2 = \mathfrak{m}$. Also folgt $\frac{\mathfrak{a}^2}{\gamma^{2(r-1)}} = \frac{\mathfrak{a}}{\gamma^{r-1}}$ oder $\mathfrak{a}^2 = \mathfrak{a} \cdot \gamma^{r-1}$. Wegen Sätzen 3,4 folgt hieraus $(\gamma^{r-1}) = \mathfrak{a}$, d. h. $\mathfrak{m} = \mathfrak{o}$, während doch $\mathfrak{m}$ gebrochen ist. Also muß Axiom (II.) gelten.

4.10 Das Integraltheorem für Polynome einer Veränderlichen. (27.9.1927)

This is the local-global theorem for roots of irreducible polynomials with coefficients in a number field. Hasse mentions that the proof was the outcome of a conversation between R. Brauer, H. Prüfer and himself in September 1927. (This conversation took place during the annual meeting of the "Deutsche Mathematiker Vereinigung" in Bad Kissingen in September 1927.) At the end Hasse writes down a counterexample showing that the result does not hold for reducible polynomials. He had obtained this counterexample from Artin. (Artin had not attended the meeting in Bad Kissingen.) Some years later Hasse published this local-global theorem in the "Mathematische Annalen" [Has32]. *The reason for publication was a paper (by Udo Wegner) where it was erroneously claimed that the said local-global theorem holds without the irreducibility assumption. Hasse corrected this statement. He first gave Artin's counterexample which he recalled from this entry, and then presented the proof from this entry.*

IV, 56

(27. IX. 27).

Satz. *Es sei $f(x)$ ein irreduzibles Polynom in einem algebraischen Zahlkörper k endlichen Grades. Dann und nur dann, wenn die Gleichung*

$$f(x) = 0 \ (\mathfrak{p})$$

für jede Primstelle $\mathfrak{p}$ von k lösbar ist, ist auch die Gleichung

$$f(x) = 0$$

in k lösbar (d. h. $f(x)$ linear).

Beweis: a.) Ist $f(x) = 0$ in k lösbar, so auch $f(x) = 0$ $(\mathfrak{p})$ für jede Primstelle $\mathfrak{p}$ von k. $\big(f(x)$ ist dann linear$\big)$.

b.) Sei $f(x) = 0$ $(\mathfrak{p})$ für jede Primstelle $\mathfrak{p}$ von k lösbar. Sei K der durch $f(x) = 0$ bestimmte Relativkörper über k, und $\overline{K}$ der zugehörige Galoissche Relativkörper, $\mathfrak{G}$ seine Gruppe. Wird $\mathfrak{G}$ durch die Permutationen der n konjugierten Körper $K^{(i)}$ zu K, wo n der Grad von $f(x)$ ist, dargestellt, so gehört K zu der Untergruppe, die das Permutationssymbol K festläßt. Der Typus der Zerlegung eines nicht in der Relativdiskriminante von K aufgehenden Primideals $\mathfrak{p}$ von k in K ist dann bekanntlich gleich dem Typus der Zyklenzerlegung

der $\mathfrak{p}$ bezüglich $\overline{K}$ zugeordneten Klasse von $\mathfrak{G}$. Nach Voraussetzung haben nun IV, 57 alle diese $\mathfrak{p}$ in K einen Primfaktor 1. Grades. In der zugeordneten Klasse von $\mathfrak{G}$ besitzt also die Zyklenzerlegung stets einen eingliedrigen Zyklus. Nach Tschebotareff (übertragen auf Relativkörper) kommt nun jede Klasse von $\mathfrak{G}$ wirklich bei unendlich vielen Primidealen $\mathfrak{p}$ vor. Somit läßt jede Permutation von $\mathfrak{G}$ mindestens ein Symbol ungeändert. Sei g die Ordnung von $\mathfrak{G}$. Da $f(x)$ irreduzibel, ist $\mathfrak{G}$ transitiv. Folglich ist die Anzahl der Elemente, die ein bestimmtes Symbol festlassen, gleich $\frac{g}{n}$. Überdecken sich diese Elementsysteme nicht, d. h. läßt jedes Element von $\mathfrak{G}$ auch *nur* eins der n Symbole fest, so liefert diese Abzählung den richtigen Wert $n \cdot \frac{g}{n}$ als Anzahl der Elemente von $\mathfrak{G}$, sonst einen kleineren. Da aber das Einheitselement alle Symbole festläßt, käme ein Widerspruch heraus, wenn nicht trivialerweise $g = 1$ ist. Also ist $g = 1$, d. h. $f(x)$ linear*).

Von der Voraussetzung wurde hierbei sogar nur der auf die Nichtdiskriminantenteiler bezügliche Teil ausgenutzt, und auch hier nur soweit, als noch endlich viele Ausnahmen zugelassen werden können.

Folgendes *Artin*sche Beispiel zeigt, daß die Voraussetzung, $f(x)$ sei *irreduzibel*, wesentlich ist:

$$f(x) = (x^2 - p)(x^2 - q)(x^2 - pq),$$

wo p, q verschiedene Primzahlen mit den (verträglichen) Eigenschaften:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = 1\,, \quad p \equiv 1 \text{ mod. } 8.$$

*) Der gruppentheoretische Schluß entstammt einer gemeinsamen Überlegung von *R. Brauer*, *H. Prüfer* und mir auf der Fahrt nach *Kissingen*, 18. IX. 27.

4.11 Reduktion der Frage betr. primitive Wurzeln. (28.9.1927)

This is a continuation of the entry of September 27, 1927 on primitive roots.]. The result is a reformulation of Artin's conjecture in terms of estimates on the order of magnitude of certain sets of prime numbers. Hasse had written this to Artin and he replied: "One should check again the whole prime number theory with $\pi(x) < ?$ *with estimates as good as possible…". See* [FR08], *section 17.2.*

IV, 58

(28. IX. 27).

Im Anschluß an S. 45] ff noch folgendes:

Um die a. S. 47] herausgeschälte Relation

$$\frac{P_q(N)}{P(N)} < \frac{c_q}{q(q-1)}, \quad \sum_q \frac{c_q}{q(q-1)} \quad \text{konvergent}$$

zu bestätigen, geht man zweckmäßig nur darauf aus ein von q und N unabhängiges c zu finden, sodaß

$$\frac{P_q(N)}{P(N)} < \frac{c}{q(q-1)}$$

für alle q, N ist. Das genügt ja. Es macht nichts aus, wenn das Argument N geändert wird:

$$\begin{aligned} \pi_q(x) &= \text{Anzahl der } p \leqq x, \text{ denen } E_q \text{ zukommt, d. h. die in} \\ & \quad\ K_q = R(\zeta_q, \sqrt[q]{a}) \text{ voll zerfallen.} \\ \pi(x) &= \text{Anzahl der} \quad p \leqq x. \end{aligned}$$

Dann ist zu zeigen:

$$\frac{\pi_q(x)}{\pi(x)} < \frac{c}{q(q-1)} \quad \text{für alle} \quad q, x.$$

Da E_q einem p nur zukommt, wenn $q|p-1$ ist, ist $\pi_q(x) = 0$ für $x \leqq q$, sodaß es genügt, die Relation für $q < x$ zu beweisen.

Nun ist bekanntlich

$$\left|\pi_q(x) - \frac{1}{(q-1)}\mathrm{Li}(x)\right| < \frac{C_q}{q(q-1)} \frac{x}{e^{\sqrt[3]{\lg x}}}$$

$$|\pi(x) - \mathrm{Li}(x)| < C \frac{x}{e^{\sqrt[3]{\lg x}}}.$$

IV, 59 Daher:

$$\left|\pi_q(x) - \frac{1}{q(q-1)}\pi(x)\right| < \frac{C + C_q}{q(q-1)}\,\frac{x}{e^{\sqrt[3]{\lg x}}}$$

$$\left|\frac{\pi_q(x)}{\pi(x)} - \frac{1}{q(q-1)}\right| < \frac{C + C_q}{q(q-1)}\,\frac{x}{\pi(x)e^{\sqrt[3]{\lg x}}} < B\frac{C + C_q}{q^2}\,\frac{\lg x}{e^{\sqrt[3]{\lg x}}}$$

wo B eine neue, von q unabhängige Konstante. Also:

$$\frac{\pi_q(x)}{\pi(x)} < \frac{1}{q(q-1)} + B\frac{C + C_q}{q(q-1)}\,\frac{\lg x}{e^{\sqrt[3]{\lg x}}}\,.$$

Um nun die rechte Seite $< \frac{x}{q(q-1)}$ zu bekommen, muß

$$1 + B(C + C_q)\frac{\lg x}{e^{\sqrt[3]{\lg x}}} < c$$

sein. Es kommt also darauf an, die Beschränktheit von $C_q \frac{\lg x}{e^{\sqrt[3]{\lg x}}}$ zu beweisen, d. h. wegen $q < x$ auf:

$$\boxed{C_q = O\left(\frac{e^{\sqrt[3]{\lg q}}}{\lg q}\right).}$$

Gilt diese Tatsache, so ist die Artinsche Formel richtig.

4.12 Eine Ostrowskische Aufgabe. (28.9.1927)

It appears that Hasse had learned this problem during the meeting of the "Deutsche Mathematiker Vereinigung" in Bad Kissingen in September 1927. Same for the problems in the next entries.

IV, 60

(28. IX. 27).

(Siehe dazu J. B. d. D. M. V. **34** (1926), S. *157* und **35** (1926), S. *89*).

„Für alle komplexen x ist $|\lg(1+x)| \geqq \lg(1+|x|)$, wo links eine beliebige Bestimmung des Logarithmus, rechts der reelle Logarithmus zu nehmen ist. Das Gleichheitszeichen gilt nur für $x = |x|$."

Beweis: Mit $\lg(1+x) = y$ lautet die Behauptung

$$|y| \geqq \lg(1 + |e^y - 1|),$$

d. h.

$$\begin{aligned} e^{|y|} &\geqq 1 + |e^y - 1| \\ |e^y - 1| &\leqq e^{|y|} - 1 \\ \left| \sum_{\nu=1}^{\infty} \frac{y^\nu}{\nu!} \right| &\leqq \sum_{\nu=1}^{\infty} \frac{|y|^\nu}{\nu!} . \end{aligned}$$

4.13 Eine Knoppsche Aufgabe. (28.9.1927)

IV, 61

(Mitgeteilt in Kissingen, September 1927)

(28. IX. 27).

„Die Ungleichung $\frac{1}{k_1} + \cdots + \frac{1}{k_n} < 1$ ist möglichst gut, d. h. mit möglichst großem Wert der linken Seite, bei gegebenem n durch natürliche Zahlen k_ν zu lösen. Vermutet wird, daß dies für jedes n durch die Folge

$$k_1 = 2, \quad k_\nu = k_1 \cdots k_{\nu-1} + 1$$

geleistet wird.“

Es ist leicht zu sehen, daß dies für $n = 2, 3, 4$ richtig ist. Ferner, daß k_n nicht besser gewählt werden kann, wenn $k_1, \ldots, k_{n-1}$ wie angegeben bestimmt sind.

Herr *Grandjot* soll im Besitz einer von anderer Seite gegebenen Lösung sein.

P. S. 4. X. 27. Auskunft *Grandjot*s: die Aufgabe rührt eigentlich von *Kellogg* her. Sie ist gelöst durch *Curtiss*, American Mathem. Monthly **29**, 380—387.

(Siehe genaue Ausarbeitung in Tagebuch V, S. 25])

4.14 Eine Brandtsche Aufgabe. (28.9.1927)

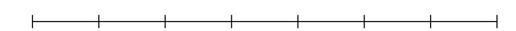
IV, 62

(Mitgeteilt von H. Brandt, Kissingen, September 1927)

(28. IX. 27).

„Einen Kreis mit Zirkel und Lineal in n inhalts– und umfangsgleiche Teile zu teilen.“

Lösung:



Die Inhalte der Teile eines Halbkreises verhalten sich wie die ersten Differenzen von

$$0^2, 1^2, 2^2, \ldots, n^2$$

d. h. wie

$$1, 3, 5, \ldots, 2n-1$$

Je zwei komplementäre zusammengenommen ergeben also inhaltsgleiche Teile.

Die Umfänge der Teile eines Halbkreises, von den nachher nicht zu berücksichtigenden geradlinigen Stücken abgesehen verhalten sich wie

$$0+1, 1+2, \ldots, (n-1)+n$$

d. h. wieder wie

$$1, 2, 3, \ldots, 2n-1.$$

Daraus folgt die Umfangsgleichheit wie eben.

4.15 v.d.Waerdens Lösung einer Baudetschen Aufgabe. (28.9.1927)

It appears that van der Waerden had talked about this topic at the DMV-meeting in Kissingen, September 1927 and Hasse had taken notes. Van der Waerden published this proof in [vdW27]. *It has been included in the book by Chintchin "Three Pearls of Number Theory"* [Chi51]. *Later van der Waerden reported how he had obtained this proof in* [vdW98].

IV, 63

(Mitgeteilt in Kissingen, September 1927)

(28. IX. 27).

Die ursprüngliche *Baudet*sche Aufgabe lautete:

> „Ist irgendeine Einteilung aller natürlichen Zahlen in 2 Klassen gegeben, so gibt es in mindestens einer der beiden Klassen eine arithmetische Progression von einer vorgeschriebenen Anzahl ℓ von Gliedern."

Zum Induktionsbeweis wird die Behauptung folgendermaßen erweitert:

> „Zu irgendzwei natürlichen Zahlen k, ℓ existiert stets ein $n_0(k,\ell)$, sodaß, wenn irgendeine Einteilung aller natürlichen Zahlen bis $n_0(k,\ell)$ in k Klassen gegeben ist, in mindestens einer Klasse eine arithmetische Progression von ℓ Gliedern vorkommt."

Beweis: Die Behauptung stimmt für $\ell = 2$ und beliebiges k, nämlich mit $n_0(k,2) = k+1$, weil bis $k+1$ sicher ein Zahlenpaar in einer der k Klassen vorkommt. Angenommen, die Behauptung sei richtig für $\ell - 1$ und beliebiges k.

IV, 64

Dann zeigen wir ihre Richtigkeit für ℓ und beliebiges k so:

Wir betrachten, wenn $n_1, \ldots, n_{k-1}$ beliebige natürliche Zahlen sind, mit deren Verwendung gebildete Systeme 1–ter, …, $(k-1)$–ter Ordnung. Unter dem System 1–ter Ordnung $S_a^{(1)}$ sei die Folge der natürlichen Zahlen $\{a, a+1, \ldots, a+(n_1-1)\}$ verstanden, unter dem System 2–ter Ordnung $S_a^{(2)}$ die Folge der Systeme 1–ter Ordnung $\{S_a^{(1)}, S_{a+1}^{(1)}, \ldots, S_{a+(n_2-1)}^{(1)}\}$, u. s. f. Dabei bedeutet a jeweils irgendeine natürliche Zahl. Ist nun eine Einteilung der natürlichen Zahlen in k Klassen gegeben, so bewirkt diese zunächst eine Einteilung der Systeme 1–ter Ordnung in k^{n_1} Klassen*), wenn nämlich $S_a^{(1)}$ und $S_b^{(1)}$ dann und nur dann in die

*) Genauer: höchstens k^{n_1} Klassen. Wir zählen aber leere Klassen in beliebiger Anzahl mit. Bezüglich der Behauptung und der Induktionsannahme macht das gar nichts aus.

gleiche Klasse gerechnet werden, wenn $a+\nu$ und $b+\nu$ für jedes $\nu = 0, 1, \ldots, n_1-1$ in derselben Klasse sind. Ebenso wird dadurch eine Einteilung aller Systeme 2–ter Ordnung in $k^{n_1 n_2}$ Klassen bewirkt, wenn nämlich $S_a^{(2)}$ und $S_b^{(2)}$ dann und nur dann in die gleiche Klasse gerechnet werden, wenn $S_{a+\nu}^{(1)}$ und $S_{b+\nu}^{(1)}$ für jedes $\nu = 0, 1, \ldots, n_2 - 1$ in derselben Klasse sind, u. s. f.Die Systeme einer Ordnung sind den natürlichen Zahlen eineindeutig zugeordnet. Es hat also einen Sinn, bei ihnen von einer arithmetischen Progression zu reden und die Induktionsannahme auf sie anzuwenden. Wir wählen nun die Längen $n_1, \ldots, n_{k-1}$ dieser Systeme folgendermaßen: IV, 65

$$n_1 \geqq \frac{\ell-1}{\ell-2} n_0(k, \ell-1), \; n_2 \geqq \frac{\ell-1}{\ell-2} n_0(k^{n_1}, \ell-1), \ldots$$
$$\ldots, n_{k-1} \geqq \frac{\ell-1}{\ell-2} n_0(k^{n_1 n_2 \ldots n_{k-2}}, \ell-1).$$

Nach der Induktionsannahme gibt es nun zunächst eine Klasse unter den Systemen $(k-1)$–ter Ordnung, in der eine arithmetische Progression $\ell - 1$ Gliedern vorkommt. Ihre Differenz sei d_{k-1}.

Wir bezeichnen sie symbolisch mit

$$S_{a_{k-1}}^{(k-1)} + \nu_{k-1} d_{k-1} \qquad (\nu_{k-1} = 0, \ldots, \ell-2).$$

In $S_{a_{k-1}}^{(k-1)}$ gibt es ferner nach Wahl von n_{k-1} eine Klasse von Systemen $(k-2)$–ter Ordnung, die eine arithmetische Progression

$$S_{a_{k-2}}^{(k-2)} + \nu_{k-2} d_{k-2} \qquad (\nu_{k-2} = 0, \ldots, \ell-2)$$

von Systemen $(k-2)$–ter Ordnung enthält. Nach Definition der Äquivalenz von Systemen sind nun, weil die Progression $(k-1)$–ter Ordnung in einer Klasse liegt, die Systeme der Progression $(k-2)$–ter Ordnung im ersten System $S_{a_{k-1}}^{(k-1)}$ in einer Klasse mit den homologen, durch Verschiebung um $\nu_{k-1} d_{k-1}$ entstehenden Systemen $(k-2)$–ter Ordnung, und weil die Systeme $(k-2)$–ter Ordnung $S_{a_{k-2}}^{(k-2)} + \nu_{k-2} d_{k-2}$ selbst in einer Klasse liegen, natürlich auch miteinander. Es gehören also zu ein– u. derselben Klasse alle Systeme: IV, 66

$$S_{a_{k-2}}^{(k-2)} + \nu_{k-2} d_{k-2} + \nu_{k-1} d_{k-1} \qquad (\nu_{k-2}, \nu_{k-1} = 0, \ldots, \ell-2).$$

Wegen des Faktors $\frac{\ell-1}{\ell-2}$ bei der Definition von n_{k-1} gehören auch noch die Systeme dieser Art mit $\nu_{k-2} = \ell - 1$ zu den $S_{a_{k-1}}^{(k-1)} + \nu_{k-1} d_{k-1}$ und sind daher

in der gleichen Klasse, aber nicht notwendig in derselben, wie die übrigen.

So fortfahrend kommt man schließlich zu einer Klasse von Systemen 0–ter Ordnung, d. h. Zahlen, die eine arithmetische Progression

$$a_0 + \nu_0 d_0 \qquad (\nu_0 = 0, \dots, \ell - 2)$$

IV, 67 von Zahlen enthält. Über den „Anfang“:

$$A(\nu_0, \dots, \nu_{k-1}) = a_0 + \nu_0 d_0 + \nu_1 d_1 + \dots + \nu_{k-2} d_{k-2} + \nu_{k-1} d_{k-1}$$

dieser Progression gilt dann nach der Konstruktion folgendes:

1.) Die Zahlen $A(\nu_0, \dots, \nu_{k-1})$ mit $\nu_0, \dots, \nu_{k-1} = 0, \dots, \ell-2$ gehören sämtlich ein– u. derselben Klasse $\mathfrak{K}_1$ an.

2.) Die Zahlen $A(\ell - 1, \nu_1, \dots, \nu_{k-1})$ mit $\nu_1, \dots, \nu_{k-1} = 0, \dots, \ell - 2$ gehören sämtlich ein– u. derselben Klasse $\mathfrak{K}_2$ an.

3.) Die Zahlen $A(\ell - 1, \ell - 1, \nu_2, \dots, \nu_{k-1})$ mit $\nu_2, \dots, \nu_{k-1} = 0, \dots, \ell - 2$ gehören sämtlich ein– u. derselben Klasse $\mathfrak{K}_3$ an.

....

k.) Die Zahlen $A(\ell - 1, \ell - 1, \dots, \ell - 1, \nu_{k-1})$ mit $\nu_{k-1} = 0, \dots, \ell - 2$ gehören sämtlich ein– u. derselben Klasse $\mathfrak{K}_k$ an.

1.) Ist $\mathfrak{K}_2 = \mathfrak{K}_1$, so enthält $\mathfrak{K}_1$ die arithmetische Progression $a_0 + \nu_0 d_0$ mit $\nu_0 = 0, \dots, \ell - 1$ von ℓ Gliedern.
2.) Ist $\mathfrak{K}_2 \neq \mathfrak{K}_1$, so kann $\mathfrak{K}_3 = \mathfrak{K}_1$ oder $\mathfrak{K}_3 = \mathfrak{K}_2$ sein. Ist $\mathfrak{K}_3 = \mathfrak{K}_1$, so enthält $\mathfrak{K}_1$ die arithmetische Progression $a_0+\nu_0(d_0+d_1)$ mit $\nu_0 = 0, \dots, \ell-1$ von ℓ Gliedern. Ist $\mathfrak{K}_3 = \mathfrak{K}_2$, so enthält $\mathfrak{K}_2$ die arithmetische Progression $a_0 + (\ell - 1)d_0 + \nu_1 d_1$ mit $\nu_1 = 0, \dots, \ell - 1$ von ℓ Gliedern.
3.) Ist $\mathfrak{K}_2 \neq \mathfrak{K}_1$ und $\mathfrak{K}_3 \neq \mathfrak{K}_1, \mathfrak{K}_2$, so kann $\mathfrak{K}_4 = \mathfrak{K}_1$ oder $\mathfrak{K}_4 = \mathfrak{K}_2$ oder $\mathfrak{K}_4 = \mathfrak{K}_3$ sein. Ist $\mathfrak{K}_4 = \mathfrak{K}_1$, so enthält $\mathfrak{K}_1$ die arithmetische Progression $a_0+\nu_0(d_0+d_1+d_2)$ mit $\nu_0 = 0, \dots, \ell-1$ von ℓ Gliedern. Ist $\mathfrak{K}_4 = \mathfrak{K}_2$, so enthält $\mathfrak{K}_2$ die arithmetische Progression $a_0 + (\ell - 1)d_0 + \nu_1(d_1 + d_2)$ mit $\nu_1 = 0, \dots, \ell - 1$ von ℓ Gliedern. Ist $\mathfrak{K}_4 = \mathfrak{K}_3$, so enthält $\mathfrak{K}_3$ die arithmetische Progression $a_0 + (\ell - 1)d_0 + (\ell - 1)d_1 + \nu_2 d_2$ mit $\nu_2 = 0, \dots, \ell - 1$ von ℓ Gliedern.

....

IV, 68 *k.*) Ist $\mathfrak{K}_2 \neq \mathfrak{K}_1, \mathfrak{K}_3 \neq \mathfrak{K}_1, \mathfrak{K}_2, \dots, \mathfrak{K}_k \neq \mathfrak{K}_1, \dots, \mathfrak{K}_{k-1}$, so muß die Zahl $A(\ell -$

$1, \ldots, \ell - 1$) doch in einer der k Klassen $\mathfrak{K}_1, \ldots, \mathfrak{K}_k$ liegen. Dann enthält diese Klasse die arithmetische Progression von ℓ Gliedern:

$$
\begin{array}{ll}
a_0 + \nu_0(d_0 + d_1 + \cdots + d_{k-1}), & \text{mit} \quad \nu_0 = 0, \ldots, \ell - 1, \\
 & \text{wenn sie } \mathfrak{K}_1 \text{ ist,} \\
a_0 + (\ell - 1)d_0 + \nu_1(d_1 + \cdots + d_{k-1}), & \text{mit} \quad \nu_1 = 0, \ldots, \ell - 1, \\
 & \text{wenn sie } \mathfrak{K}_2 \text{ ist,} \\
\cdots\cdots\cdots & \\
a_0 + (\ell - 1)d_0 + \cdots + (\ell - 1)d_{k-2} + \nu_{k-1}d_{k-1}, & \text{mit} \quad \nu_{k-1} = 0, \ldots, \ell - 1, \\
 & \text{wenn sie } \mathfrak{K}_k \text{ ist,}
\end{array}
$$

Damit sind alle Möglichkeiten erschöpft und daher ist der Beweis erbracht. Es erübrigt sich, die nach dem Beweis jedenfalls, wie für die Induktion erforderlich, nicht von der Klasseneinteilung abhängige Grenze $n_0(k, \ell)$ abzuschätzen. Zu dem Zweck bemerken wir zunächst, daß die obigen Abschätzungen (S. 65]) wie folgt verschärft werden können:

$$
\begin{array}{rcl}
n_1 & = & n_0(k, \ell - 1) + \left[\frac{n_0(k,\ell-1)-1}{\ell-2}\right] \\
n_2 & = & n_0(k^{n_1}, \ell - 1) + \left[\frac{n_0(k^{n_1},\ell-1)-1}{\ell-2}\right] \\
\cdots & \cdots & \cdots \\
n_{k-1} & = & n_0(k^{n_1 \cdots n_{k-2}}, \ell - 1) + \left[\frac{n_0(k^{n_1 \cdots n_{k-2}},\ell-1)-1}{\ell-2}\right].
\end{array}
$$

Für die Differenzen $d_0, \ldots, d_{k-1}$ hat man ferner

$$
\begin{array}{rcl}
d_0 & \leqq & \left[\frac{n_0(k,\ell-1)-1}{\ell-2}\right] \\
d_1 & \leqq & \left[\frac{n_0(k^{n_1},\ell-1)-1}{\ell-2}\right] \\
\cdots & \cdots & \cdots \\
d_{k-1} & \leqq & \left[\frac{n_0(k^{n_1 \cdots n_{k-1}},\ell-1)-1}{\ell-2}\right].
\end{array}
$$

Dies bezieht sich natürlich durchweg nur auf $\ell > 2$, während der triviale Fall $\ell = 2$ als Ausgangspunkt für die Rekursion zu nehmen ist. Da die maximal weit erstreckte Progression von ℓ Gliedern beim Beweis das letzte Glied

IV, 69

$$a_0 + (\ell - 1)d_0 + \cdots + (\ell - 1)d_{k-1}$$

hat, ist also nur noch a_0 nach oben abzuschätzen. Man hat nun ersichtlich

$$
\begin{array}{rcl}
a_{k-1} & \leqq & n_0\,(k^{n_1 \cdots n_{k-1}}, \ell - 1) - (\ell - 2)d_{k-1} \\
a_{k-2} & \leqq & a_{k-1} + (n_{k-1} - 1) - (\ell - 2)d_{k-2} \\
\cdots & \cdots & \cdots \\
a_0 & \leqq & a_1 + (n_1 - 1) - (\ell - 2)d_0.
\end{array}
$$

Das ergibt also:

$$\begin{aligned} n_0(k,\ell) \leqq & n_0\left(k^{n_1\cdots n_{k-1}}, \ell-1\right) + (n_{k-1}-1) + \cdots + (n_1-1) \\ & - (\ell-2)(d_0+\cdots+d_{k-1}) + (\ell-1)(d_0+\cdots+d_{k-1}) \\ n_0(k,\ell) \leqq & n_0\left(k^{n_1\cdots n_{k-1}}, \ell-1\right) + (n_{k-1}-1) + \cdots + (n_1-1) \\ & + (d_0+\cdots+d_{k-1}), \end{aligned}$$

und somit als mögliche Wahl

$$\begin{aligned} n_0(k,\ell) = & n_0\left(k^{n_1\cdots n_{k-1}}, \ell-1\right) + n_0\left(k^{n_1\cdots n_{k-2}}, \ell-1\right) + \cdots + n_0\left(k, \ell-1\right) \\ & - (k-1) + \left[\frac{n_0\left(k^{n_1\cdots n_{k-1}}, \ell-1\right)-1}{\ell-2}\right] \\ & + 2\left(\left[\frac{n_0\left(k^{n_1\cdots n_{k-2}}, \ell-1\right)-1}{\ell-2}\right] + \cdots + \left[\frac{n_0\left(k, \ell-1\right)-1}{\ell-2}\right]\right), \end{aligned}$$

wo die Exponenten $n_1, \ldots, n_{k-1}$ sich nach S. 68] bestimmen, und wo die Rekursion nach ℓ mit

$$n_0(k,2) = k+1$$

beginnt.

Kapitel 5

Tagebuch V: Oktober 1927 – Juli 1928

Eintragungen

5.1 Ein Satz über das m–te Normenrestsymbol. (3.10.1927)

Hasse verifies the formula describing the behavior of the Hilbert norm symbol with respect to addition. Today this is well known, and in the case of a prime exponent ℓ it was also well known to Hasse. But we note that the norm residue symbol as considered here belongs to an arbitrary exponent m. The possibility of dealing with an arbitrary exponent arose after Artin had obtained his general reciprocity law. That had happened three months prior to this entry, in July 1927. Artin had immediately informed Hasse about his achievement. They had then arranged that Hasse should develop the general theory of the norm symbol, based on Artin's reciprocity law. Hasse did so and his paper appeared in 1927 in Crelle's Journal [Has27b]*, almost at the same time as the appearance of Artin's paper in the "Hamburger Abhandlungen"* [Art27]. *But the formula as given here does not appear in the cited paper of Hasse. Instead, it appears in Hasse's later paper of 1929 on the explicit reciprocity law* [Has29]. *The proof given there in §1 is almost verbatim the same as in this entry. We can regard this entry as the blueprint of §1 of that paper. The rest of that paper is modeled after the next entry.]*

V, 3

(3. X. 1927).

Sei k ein algebraischer Zahlkörper, der die m–ten Einheitswurzeln enthält und α, β, γ irgend drei Zahlen $\neq 0$ aus k, die durch die Relation

$$\alpha + \beta = \gamma$$

verbunden sind. Bezeichnet dann $(\ldots,\ldots)_m$ das m–te Normenrestsymbol nach irgendeiner Primstelle von k, so gilt die Relation

$$(\alpha, \beta)_m = (\alpha, \gamma)_m (\gamma, \beta)_m (-1, \gamma)_m \,.$$

Beweis: Sei zunächst ξ eine beliebige Zahl $\neq 0, 1$ aus k, und sei

$$\xi = \xi_0^{\mu} \qquad (m = \mu\overline{\mu})$$

mit maximalem μ, sodaß $k(\sqrt[m]{\xi}) = k(\sqrt[\overline{\mu}]{\xi_0})$ vom Grade $\overline{\mu}$ über k ist. Bezeichnet N die Relativnorm von diesem Körper nach k, so ist

$$N(1 - \sqrt[\overline{\mu}]{\xi_0}) = 1 - \xi_0$$

und folglich

$$(1-\xi_0, \xi_0)_{\overline{\mu}} = 1.$$

Bezeichnet nun ζ_μ eine beliebige μ–te Einheitswurzel, und ersetzt man hierin ξ_0 durch $\zeta_\mu \xi_0$, so darf im rechten Glied wieder einfach ξ_0 gesetzt werden, weil ja ζ_μ eine $\overline{\mu}$–te Potenz in k ist. Somit ist auch

$$(1-\zeta_\mu \xi_0, \xi_0)_{\overline{\mu}} = 1$$

für jedes ζ_μ . Daraus folgt V, 4

$$(1-\xi, \xi)_m = (1-\xi_0^\mu, \xi_0^\mu)_m = (1-\xi_0^\mu, \xi_0)_{\overline{\mu}} = \prod_{\zeta_\mu} (1-\zeta_\mu \xi_0, \xi_0) = 1.$$

(**Einfacher** lautet der bisherige Schluß so: Weil $1-\zeta_\mu \xi_0$ für jedes ζ_μ Relativnorm aus $k(\sqrt[\overline{\mu}]{\xi_0}) = k(\sqrt[m]{\xi})$ ist, gilt dasselbe auch für $1-\xi = \prod_{\zeta_\mu}(1-\zeta_\mu \xi_0)$.)

Setzen wir nun $\frac{\beta}{\gamma} = \xi$, sodaß $\frac{\alpha}{\gamma} = 1-\xi$ ist, so folgt

$$\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right)_m = 1,$$

also

$$(\alpha, \beta)_m (\alpha, \gamma)_m^{-1} (\gamma, \beta)_m^{-1} (\gamma, \gamma)_m = 1$$
$$(\alpha, \beta)_m = (\alpha, \gamma)_m (\gamma, \beta)_m (\gamma, \gamma)_m^{-1}.$$

Es sei nun

$$\gamma = \gamma_0^\mu \qquad (m = \mu\overline{\mu})$$

mit maximalem μ, und N bezeichne die Relativnorm aus $k(\sqrt[m]{\gamma}) = k(\sqrt[\overline{\mu}]{\gamma_0})$. Dann ist, wenn $\zeta_{\overline{\mu}}$ eine primitive $\overline{\mu}$–te Einheitswurzel ist,

$$\begin{aligned} N(\sqrt[\overline{\mu}]{\gamma_0}) &= \zeta_{\overline{\mu}}^{\frac{\overline{\mu}(\overline{\mu}-1)}{2}} \gamma_0 = (-1)^{\overline{\mu}-1}\gamma_0 \\ N(\sqrt[\overline{\mu}]{\gamma_0}^{\,\mu}) &= \zeta_{\overline{\mu}}^{\frac{m(\overline{\mu}-1)}{2}} \gamma = (-1)^{\mu(\overline{\mu}-1)}\gamma = (-1)^{\mu\overline{\mu}}(-1)^{\mu-1}(-\gamma) \end{aligned}$$

Nun ist erstens $(-1)^{\mu\overline{\mu}} = N(-1)^\mu$. Zweitens ist auch $(-1)^{\mu-1}$ stets Relativnorm; für ungerades μ ist das klar, ebenso für gerades μ und ungerades $\overline{\mu}$; sind aber μ und $\overline{\mu}$ beide gerade, so enthält ja k eine primitive $2\overline{\mu}$–te Einheitswurzel $\zeta_{2\overline{\mu}}$

V, 5 und es ist $-1 = \zeta_{2\overline{\mu}}^{\overline{\mu}}$ wieder Relativnorm. Zusammengenommen folgt also, daß $-\gamma$ stets Relativnorm aus $k(\sqrt[m]{\gamma})$ ist. Daher ist

$$(\gamma, \gamma)_m^{-1} = (-\gamma, \gamma)_m^{-1}(-1, \gamma)_m^{-1} = (-1, \gamma)_m^{-1} = (-1, \gamma)_m \,,$$

was die Behauptung ergibt.

Für ungerades m kann natürlich der Zusatzfaktor $(-1, \gamma)_m$ weggelassen werden.

(**Einfacher** lautet der Schluß über $(-1)^{\mu-1}$ so: Es ist stets $(-1)^{\mu-1} = N\left(\zeta_{2\overline{\mu}}^{\mu-1}\right)$. Denn $\zeta_{2\overline{\mu}}^{\mu-1}$ ist ersichtlich stets in k und $N\left(\zeta_{2\overline{\mu}}^{\mu-1}\right) = \zeta_{2\overline{\mu}}^{\overline{\mu}(\mu-1)} = \zeta_2^{\mu-1} = (-1)^{\mu-1}$. Demgemäß ist also stets

$$-\gamma = N\left((-1)^{\mu}\zeta_{2\overline{\mu}}^{\mu-1}\sqrt[\overline{\mu}]{\gamma_0}^{\mu}\right).)$$

5.2 Zum expliziten Reziprozitätsgesetz im Körper der ℓ^n–ten Einheitswurzeln. (4.10.1927)

This is the attempt of Hasse to deduce explicit formulas for the reciprocity law with respect to an arbitrary prime power ℓ^n, in the field of ℓ^n-th roots of unity. He uses the Hilbert symbol which he had defined in his paper [Has27b] *on the basis of Artin's general reciprocity law. The method in this entry goes back to Eisenstein* [Eis50]*. It was Artin who had pointed out Eisenstein's method to Hasse. Although Hasse was able to obtain explicit formulas he was not quite satisfied because there appeared a certain operator* S *which is not canonical.] Therefore Hasse postponed publication while trying to get better formulas. Apparently he did not succeed, and one year later, in November 1928, he sent his manuscript with essentially the same formulas to Artin who accepted it for the "Hamburger Abhandlungen"* [Has29]. *See also* [FR08]*, section 17.3. See also the entry of October 16, 1928.].*

V, 6

(4. X. 27).

(Siehe hierzu weitgehend schon *Eisenstein*, Crelle **39** (1850), S. 351–364).

Sei ℓ^n eine *ungerade* Primzahlpotenz, ζ_n eine primitive ℓ^n–te Einheitswurzel, $\lambda_n = 1 - \zeta_n$ der Primteiler von ℓ im Körper k_n der ℓ^n–ten Einheitswurzeln.

Ich setze für jedes $a \geqq 1$

$$\eta_a = 1 - \lambda_n^a.$$

Dann gilt ersichtlich

$$\eta_{a+b} = \eta_b + \lambda_n^b \eta_a.$$

Bezeichnet also (η_a, η_b) den Umkehrfaktor für das ℓ^n–te Potenzrestsymbol in k_n, d. h. als Normenrestsymbol geschrieben:

$$(\eta_a, \eta_b) = \left(\frac{\eta_a, \eta_b}{\lambda_n}\right)^{-1},$$

so gilt nach dem in der vorigen Eintragung bewiesenen Satz

$$(\lambda_n^b \eta_a, \eta_b) = (\lambda_n^b \eta_a, \eta_{a+b})(\eta_{a+b}, \eta_b),$$

also

$$(\eta_a, \eta_b) = (\eta_a, \eta_{a+b})(\eta_{a+b}, \eta_b)(\lambda_n, \eta_{a+b})^b (\lambda_n^b, \eta_b)^{-1}.$$

Da λ_n prim zu den η ist, gilt nach der Produktformel

$$(\lambda_n, \eta_{a+b}) = \left(\frac{\lambda_n}{\eta_{a+b}}\right), \quad (\lambda_n^b, \eta_b) = \left(\frac{\lambda_n^b}{\eta_b}\right) = \left(\frac{\lambda_n^b}{1-\lambda_n^b}\right) = 1.$$

Folglich ist

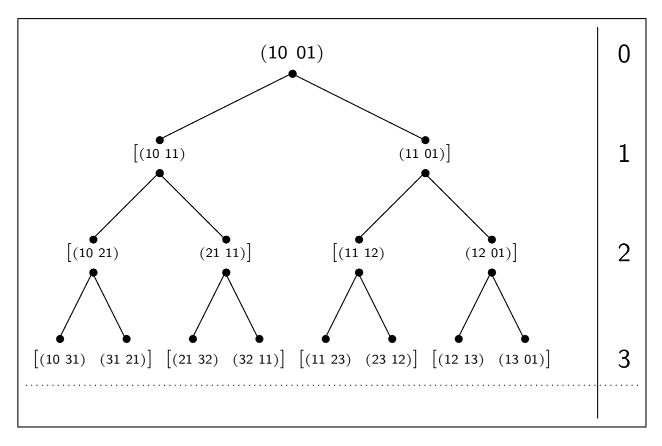
$$(\eta_a, \eta_b) = (\eta_a, \eta_{a+b})(\eta_{a+b}, \eta_b)\left(\frac{\lambda_n}{\eta_{a+b}}\right)^b,$$

und hierin ist auch noch der Zusatzfaktor $\left(\frac{\lambda_n}{\eta_{a+b}}\right)^b = 1$, wenn $a+b$ prim zu ℓ ist.
V, 7 Wenn diese Formel iteriert wird, bis die rechts auftretenden Umkehrfaktoren sämtlich eine ℓ^n–primäre Komponente enthalten, so entsteht:

$$(\eta_a, \eta_b) = \prod_{p,q}\left(\frac{\lambda_n}{\eta_{pa+qb}}\right)^{p'a+q'b}.$$

Es handelt sich jetzt um die Bestimmung derjenigen Paare positiver ganzer p, q, die hier auftreten. Von diesen brauchen dann immer nur die beibehalten zu werden, für die $pa + qb \equiv 0 \mod. \ell$ ist.

Da der Übergang von (a, b) zu $(a, a+b)$ und $(a+b, b)$ je eine Modulsubstitution ist, entstehen jedenfalls nur teilerfremde Paare p, q. Wir haben nun das folgende System für die Entstehung der Zahlenpaare p, q:



Dabei stehen in der 0–ten Zeile (Numerierung rechts) die beiden Ausgangspaare (10 01) entsprechend $(1a + 0b, 0a + 1b)$, dann in der 1–ten Zeile die $\big[(1a + 0b, 1a + 1b)\ (1a + 1b, 0a + 1b)\big]$ entsprechenden Paare, u. s. f. Je zwei

zusammengehörige Paare, die durch runde Klammern verbunden sind, mögen ein „Quadrupel“ heißen und je zwei Quadrupel mit demselben „Stammquadrupel“, die durch eckige Klammern verbunden sind, ein „Biquadrupel“. Ich beweise nun folgendes über die in der r–ten Zeile stehenden Biquadrupel V, 8

$$\big[(p''q''\ pq)\ (pq\ p'q')\big],$$

wo

$$p = p'' + p' \qquad q = q'' + q'$$

ist:

Die Zahlenpaare p, q durchlaufen alle und nur diejenigen Paare positiver ganzer teilerfremder Zahlen, für die der gewöhnliche Kettenbruch

$$\frac{p}{q} = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_\nu}} = [a_1, \ldots, a_\nu] \qquad (a_1 \geqq 0, a_2 \geqq 1, \ldots)$$

gerade die Quersummen

$$a_1 + \cdots + a_\nu = r$$

hat. (Das ist unabhängig von der Zweideutigkeit der Kettenbruchentwicklung von $\frac{p}{q}$, die ja stets mit einer geraden oder mit einer ungeraden Anzahl ν von Teilnennern geschrieben werden kann, indem man einen Schlußnenner 1 beifügt oder wegschafft). Ferner sind dabei $\frac{p'}{q'}$ und $\frac{p''}{q''}$ die vorletzten Näherungsbrüche, und zwar $\frac{p'}{q'}$ bei gerader, $\frac{p''}{q''}$ bei ungerader Teilernenneranzahl ν, wodurch dann p', q' und p'', q'' eindeutig bestimmt sind.

Die Reihenfolge bestimmt sich nach abnehmender Größe von $\frac{p}{q}$ (und zwar sogar inkl. der $\frac{p'}{q'}, \frac{p''}{q''}$)

Wir beweisen diese Behauptungen durch Induktion nach r. Für $r = 1$ gibt es nur die beiden Zerlegungen V, 9

$$1 = 1 = 0 + 1$$

mit den erforderlichen Bedingungen, die den beiden Darstellungen

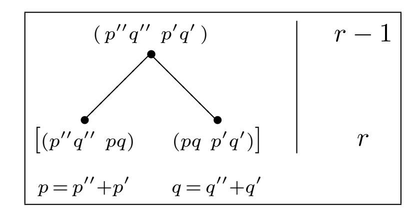
$$\frac{1}{1} = [1] = [0, 1]$$

entsprechen. Die zugehörigen Schemata für die Näherungsbrüche lauten

$$\begin{array}{cc|c} & & 1 \\ \hline 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \qquad \begin{array}{cc|cc} & & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{array}$$

Demgemäß sind die Behauptungen für $r = 1$ richtig.

Seien sie schon für $r-1$ bewiesen ($r > 1$). Dann betrachten wir die Entstehung eines Biquadrupels der r–ten Zeile aus seinem Stammquadrupel:



und unterscheiden die beiden Fälle, daß p', q' oder p'', q'' in der Mitte des Biquadrupels der $(r-1)$–ten Zeile steht.

a.) *p', q' steht in der Mitte des Biquadrupels der $(r-1)$–ten Zeile.*

Es bezeichne matrizenmäßig:

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_a = \begin{pmatrix} 0 & 1 \\ 1 & a \end{pmatrix}$$

V, 10 Vordere bezw. hintere Multiplikation mit T bedeutet Zeilen– bezw. Spalten–Vertauschung.

Nach Annahme hat der Kettenbruch mit *ungerader* Teilnennerzahl:

$$\frac{p'}{q'} = [a_1, \dots, a_{2\nu-1}]$$

die Quersumme

$$a_1 + \dots + a_{2\nu-1} = r - 1$$

und den vorletzten Näherungsbruch $\frac{p''}{q''}$. Bekanntlich bedeutet das die Matrizengleichung

$$\begin{pmatrix} p'' & p' \\ q'' & q' \end{pmatrix} = T A_{a_1} \dots A_{a_{2\nu-1}}.$$

Daraus folgt:

$$\begin{aligned}
\begin{pmatrix} p'' & p \\ q'' & q \end{pmatrix} &= \begin{pmatrix} p'' & p''+p' \\ q'' & q''+q' \end{pmatrix} = \begin{pmatrix} p'' & p' \\ q'' & q' \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= TA_{a_1} \dots A_{a_{2\nu-1}} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = TA_{a_1} \dots A_{a_{2\nu-2}} \begin{pmatrix} 0 & 1 \\ 1 & a_{2\nu-1} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= TA_{a_1} \dots A_{a_{2\nu-2}} \begin{pmatrix} 0 & 1 \\ 1 & a_{2\nu-1}+1 \end{pmatrix} = TA_{a_1} \dots A_{a_{2\nu-2}} A_{a_{2\nu-1}+1} \\
\begin{pmatrix} p' & p \\ q' & q \end{pmatrix} &= \begin{pmatrix} p' & p''+p' \\ q' & q''+q' \end{pmatrix} = \begin{pmatrix} p'' & p' \\ q'' & q' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\
&= TA_{a_1} \dots A_{a_{2\nu-1}} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = TA_{a_1} \dots A_{a_{2\nu-1}} A_1 \,,
\end{aligned}$$

also die Relationen

$$\frac{p}{q} = [a_1, \dots, a_{2\nu-2}, a_{2\nu-1}+1] = [a_1, \dots, a_{2\nu-1}, 1]$$

mit den Quersummen r und den vorletzten Näherungsbrüchen $\frac{p''}{q''}$ bezw. $\frac{p'}{q'}$, gerade in der Weise, wie behauptet. V, 11

b.) *p'', q'' steht in der Mitte des Biquadrupels der $(r-1)$–ten Zeile.*

Nach Annahme hat dann der Kettenbruch mit *gerader* Teilnennerzahl

$$\frac{p''}{q''} = [a_1, \dots, a_{2\nu}]$$

die Quersumme

$$a_1 + \dots + a_{2\nu} = r - 1$$

und den vorletzten Näherungsbruch $\frac{p'}{q'}$. Also ist jetzt

$$\begin{pmatrix} p' & p'' \\ q' & q'' \end{pmatrix} = TA_{a_1} \dots A_{a_{2\nu}} .$$

Daraus folgt ähnlich wie vorher:

$$\begin{aligned}
\begin{pmatrix} p'' & p \\ q'' & q \end{pmatrix} &= \begin{pmatrix} p'' & p''+p' \\ q'' & q''+q' \end{pmatrix} = \begin{pmatrix} p' & p'' \\ q' & q'' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\
&= TA_{a_1} \dots A_{a_{2\nu}} A_1 \\
\begin{pmatrix} p' & p \\ q' & q \end{pmatrix} &= \begin{pmatrix} p' & p''+p' \\ q' & q''+q' \end{pmatrix} = \begin{pmatrix} p' & p'' \\ q' & q'' \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\
&= TA_{a_1} \dots A_{a_{2\nu-1}} A_{a_{2\nu}+1},
\end{aligned}$$

also die Relationen

$$\frac{p}{q} = [a_1, \ldots, a_{2\nu}, 1] = [a_1, \ldots, a_{2\nu-1}, a_{2\nu} + 1]$$

mit der Quersumme r und den vorletzten Näherungsbrüchen $\frac{p''}{q''}$ bezw. $\frac{p'}{q'}$, gerade
V, 12 in der Weise, wie es sein soll.

Da ferner in beiden Fällen nach Annahme $\frac{p''}{q''} > \frac{p'}{q'}$ ist, folgt ohne weiteres

$$\frac{p''}{q''} > \frac{p}{q} > \frac{p'}{q'},$$

was die Behauptung über die Reihenfolge ergibt, wenn man bedenkt, daß $\frac{p''}{q''}$ für das vorangehende Biquadrupel der r–ten Zeile die Rolle von $\frac{p'}{q'}$, und $\frac{p'}{q'}$ für das nachfolgende Biquadrupel der r–ten Zeile die Rolle von $\frac{p''}{q''}$ übernimmt.

Es bleibt also nur noch zu zeigen, daß wirklich *jedes* Paar p, q mit Kettenbruchquersumme r in der r–ten Zeile vorkommt. Auch das folgt aus der vorstehenden Induktion. Denn der Kettenbruch $\frac{p}{q}$ läßt sich stets in einer (und nur einer) der beiden Formen a. S. 10] o. 11] unten schreiben, je nachdem er, auf den Schlußnenner 1 gebracht, eine gerade oder ungerade Teilnennerzahl hat. Da aber in der $(r-1)$–ten Zeile nach Annahme das Paar p', q' mit $\frac{p'}{q'} = [a_1, \ldots, a_{2\nu-1}]$ bezw. p'', q'' mit $\frac{p''}{q''} = [a_1, \ldots, a_{2\nu}]$ als mittleres Paar vorkommt, folgt dann das Vorkommen von p, q als mittleres Paar in der r–ten Zeile, eben nach obigen Rechnungen.

Es sei noch bemerkt, daß p, q als mittleres Paar eines Biquadrupels auch an *nur* einer Stelle des Schemas vorkommt. Denn die Zeile ist durch die Quersumme des Kettenbruchs $\frac{p}{q}$ eindeutig bestimmt, und die Stelle dann durch die Größe
V, 13 des Bruchs $\frac{p}{q}$.

Ich kehre jetzt zu der Formel a. S. 7] oben zurück. Durch das Vorhergehende ist gezeigt, daß dort p, q alle Paare positiver, ganzer teilerfremder Zahlen durchlaufen und p', q' jedesmal den vorletzten Näherungsbruch $\frac{p'}{q'}$ bei Entwicklung von $\frac{p}{q}$ in einen Kettenbruch

$$\frac{p}{q} = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{2\nu}}} = [a_1, \ldots, a_{2\nu}]$$

mit gerader Teilnenneranzahl.

Unter Anwendung der Ergebnisse meiner gemeinsamen Note mit *Artin* (Hamb. Nachr.) folgt dann

$$(\eta_a, \eta_b) = \zeta_n^{\frac{1}{\ell^n} S_n \left(-\frac{\zeta_n}{\lambda_n} \sum_{p,q} (p'a+q'b) \log \eta_{pa+qb}\right)},$$

oder auch

$$(\eta_a, \eta_b) = \zeta_n^{-\sum_{(m,\ell)=1} \frac{1}{m^2} \sum_{p,q} \frac{p'a+q'b}{pa+qb} \sum_{\mu \equiv 0 (\ell^n)} (-1)^\mu \mu \binom{(pa+qb)m}{\mu}},$$

wo über die oben genannten p, q nebst den zugehörigen p', q' zu summieren ist. Es kann über *alle* diese p, q summiert werden, oder aber auch nur über solche für die

$$pa + qb \equiv 0 \mod. \ell$$

ist. Die Summation über m braucht ferner nur über das Intervall

$$\ell^n \leqq m(pa + qb) \leqq n\ell^n - (n-1)\ell^{n-1}$$

erstreckt zu werden, wodurch dann auch die Summation über p, q auf endlich viele Paare beschränkt wird. V, 14

In der Formel a. S. 7] oben kann wegen $\left(\frac{\lambda_n}{\eta_{a+b}}\right)^b = \left(\frac{\lambda_n}{\eta_{a+b}}\right)^{-a}$, weil ja $\lambda_n^a \lambda_n^b = \lambda_n^{a+b} \equiv 1 \mod. \eta_{a+b}$ ist, auch $-(p''a + q''b)$ statt $+(p'a + q'b)$ geschrieben werden, sodaß also in Änderung der Bezeichnungen auch $(-1)^\nu (p'a + q'b)$ statt $p'a + q'b$ geschrieben werden kann, wo p', q' sich aus p, q durch *beliebige* Kettenbruchentwicklung bestimmen *und ν die Anzahl der Teilnenner bezeichnet, d. h. bekanntlich* $(-1)^\nu = \left|p_q p'_{q'}\right|$.

V, 15

So erhalten wir also:

$$(\eta_a, \eta_b) = \zeta_n^{-\sum_{p,q} (-1)^\nu \frac{p'a+q'b}{pa+qb} \sum_{(m,\ell)=1} \frac{1}{m^2} \sum_{\mu \equiv 0\, (\ell^n)} (-1)^\mu \mu \binom{m(pa+qb)}{\mu}},$$

summiert über alle teilerfremden positiven p, q und alle zu ℓ primen positiven m mit

$$pa + qb \equiv 0 \mod. \ell$$
$$\ell^n \leqq m(pa + qb) \leqq n\ell^n - (n-1)\ell^{n-1},$$

wobei jedesmal $\frac{p'}{q'}$ der vorletzte Näherungsbruch von $\frac{p}{q}$ und $(-1)^\nu = \begin{vmatrix} p & p' \\ q & q' \end{vmatrix}$.

Schließlich kann man noch m in p, q hineinziehen:

$$(\eta_a, \eta_b) = \zeta_n^{-\sum_{p,q} \frac{1}{\left|\begin{smallmatrix} p & p' \\ q & q' \end{smallmatrix}\right|} \cdot \frac{p'a+q'b}{pa+qb} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \mu \binom{pa+qb}{\mu}},$$

summiert über alle Paare positiver p, q mit $(p, q, \ell) = 1$ und

$$pa + qb \equiv 0 \text{ mod. } \ell$$
$$\ell^n \leqq pa + qb \leqq n\ell^n - (n-1)\ell^{n-1},$$

V, 16 wobei jedesmal $\frac{p'}{q'}$ der vorletzte (voll gekürzte) Näherungsbruch von $\frac{p}{q}$ ist.

Man sieht dieser Formel die triviale Tatsache

$$(\eta_a, \eta_a) = 1$$

an. Für $a = b$ genügen nämlich immer gleichzeitig p, q und q, p den letzten Bedingungen. Ist nun erstens $p \neq q$ und etwa $p > q$, so ist

$$\begin{aligned} \frac{p}{q} &= [a_1, \ldots, a_\nu] \qquad a_1 \geqq 1 \\ \frac{q}{p} &= [0, a_1, \ldots, a_\nu]. \end{aligned}$$

Da dann

$$\begin{pmatrix} p' & p \\ q' & q \end{pmatrix} \sim TA_{a_1} \ldots A_{a_\nu} = A_0 A_{a_1} \ldots A_{a_\nu}$$

ist, folgt durch vordere Multiplikation mit T:

$$\begin{pmatrix} q' & q \\ p' & p \end{pmatrix} \sim TA_0 A_{a_1} \ldots A_{a_\nu}$$

sodaß q', p' zu q, p gehört, wenn p', q' zu p, q gehört. Da für je zwei solche Lösungen p, q und q, p alle Glieder im Exponenten, die Determinanten aber nur bis aufs Vorzeichen, übereinstimmen, heben sich alle solchen Glieder weg. Ist zweitens $p = q$, so ist etwa $(p', q') = (1, 0)$ und im Exponenten stets

$$\frac{1}{p} \cdot \frac{a}{2pa} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \mu \binom{2pa}{\mu}.$$

Da hier der störende Nenner a sich heraushebt, während p ja prim zu ℓ ist

V, 17 $\big((p, p, \ell) = 1\big)$, ist das $\equiv 0$ mod. ℓ^n, fällt also ebenfalls heraus. *Speziell für*

$n = 1$ erhält man einfach:

$$(\eta_a, \eta_b) = \zeta_1^{\sum_{p,q} \frac{p'a+q'b}{\left|\begin{smallmatrix} p & p' \\ q & q' \end{smallmatrix}\right|}},$$

summiert über *alle positiven* Lösungen p, q von

$$pa + qb = \ell$$

und den vorletzten Näherungsbruch $\frac{p'}{q'}$ von $\frac{p}{q}$. Wir können das so umformen:

Aus

$$\begin{aligned} pa + qb &\equiv \ell \equiv 0 \text{ mod. } \ell \\ pq' - qp' &= \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \end{aligned}$$

folgt

$$\begin{aligned} p(p'a + q'b) &\equiv b \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \text{ mod. } \ell \\ q(p'a + q'b) &\equiv -a \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} \text{ mod. } \ell \end{aligned}$$

also, da p, q von selbst prim zu ℓ sind, ebenso $\begin{vmatrix} p & p' \\ q & q' \end{vmatrix}$,

$$\frac{p'a + q'b}{\left|\begin{smallmatrix} p & p' \\ q & q' \end{smallmatrix}\right|} \equiv \frac{b}{p} \equiv -\frac{a}{q} \text{ mod. } \ell.$$

Folglich gilt:

$$(\eta_a, \eta_b) = \zeta_1^{\sum \frac{b}{p}} = \zeta_1^{-\sum \frac{a}{q}},$$

summiert über *alle positiven* Lösungen p, q von

$$pa + qb = \ell.$$

Diese Formel ist zur schnellen numerischen Berechnung der Umkehrfaktoren (η_a, η_b) im Falle $n = 1$ besonders geeignet. Die Summationsbedingung V, 18

$$pa + qb = \ell$$

läßt sich noch vereinfachen. Wir unterscheiden zwei Fälle:

1.) $(a, b) > 1$.

Dann gibt es keine Lösungen p, q. Folglich gilt:

$$(\eta_a, \eta_b) = 1, \quad \text{wenn} \quad (a, b) > 1 \qquad (n = 1).$$

2.) $(a, b) = 1$.

Dann sei a_0, b_0 die kleinste positive Lösung von

$$ba_0 - ab_0 = 1, \quad \text{also} \quad \left\{ \begin{array}{l} 0 \leqq a_0 < a \\ 0 \leqq b_0 < b \end{array} \right\}.$$

Ist dann p, q eine Lösung, so folgt

$$a(p + b_0\ell) + b(q - a_0\ell) = ap + bq - (ba_0 - ab_0)\ell = 0,$$

also die Existenz eines ganzen r, sodaß

$$\begin{array}{rcl} p + b_0\ell & = & rb \qquad \left(\text{also} \ \ \dfrac{b}{p} \equiv \dfrac{1}{r} \ \text{mod.}\, \ell\right) \\ -q + a_0\ell & = & ra \end{array}$$

ist. Für dies r gilt dann, weil $p, q > 0$ sind,

$$\frac{b_0}{b}\ell < r < \frac{a_0}{a}\ell.$$

Umgekehrt folgt aus der Existenz einer ganzen Zahl r in diesem Intervall die Existenz zweier positiver p, q mit $pa + qb = \ell$. Und die p, q sind den r eineindeutig zugeordnet. Folglich gilt

$$(\eta_a, \eta_b) = \zeta_1^{\sum \frac{1}{r}}, \quad \text{wenn} \quad (a, b) = 1 \qquad (n = 1),$$

summiert über alle ganzen r im Intervall

$$\frac{b_0}{b}\ell < r < \frac{a_0}{a}\ell, \quad \text{wobei} \quad ba_0 - ab_0 = 1, \quad \left\{ \begin{array}{l} 0 \leqq a_0 < a \\ 0 \leqq b_0 < b \end{array} \right\}.$$

V, 19

Ich will jetzt *speziell für* $n = 1$ aus den vorstehenden Formeln meine frühere allgemeine Formel herleiten (Crelle **154**, S. 105). Das braucht natürlich nur für

die Umkehrfaktoren (η_a, η_b) zu geschehen. Dazu bemerke ich, daß für positive p, q gilt

$$\binom{pa+qb-1}{\ell-1} \quad \begin{cases} =0 & \text{für} \quad pa+qb<\ell \\ =1 & \text{für} \quad pa+qb=\ell \\ \equiv 0 \text{ mod. } \ell & \text{für} \quad pa+qb>\ell. \end{cases}$$

Da die Formel, auf die ich hinaus will, für $a = 1$ oder $b = 1$ trivial ist, *werde* $a > 1$ *und* $b > 1$ *vorausgesetzt.* Es durchlaufe dann zunächst p, q alle positiven ganzen Zahlen mit

$$1 \leqq pa \leqq \ell - 1, \quad 1 \leqq qb \leqq \ell - 1,$$

sodaß insbesondere p, q prim zu ℓ sind. nach S. 17] unten und dem eben Gesagten ist dann

$$(\eta_a, \eta_b) = \zeta_1^{L(a,b)}$$

mit

$$L(a,b) \equiv \sum_{p,q} \frac{b}{p} \binom{pa+qb-1}{\ell-1} \text{ mod. } \ell.$$

Mit einer bekannten, auch im „leeren“ Gebiet gültigen Binomialkoeffizientenformel ist aber

$$\begin{aligned} \binom{pq+qb-1}{\ell-1} &= \sum_{k=0}^{qb-1} \binom{pa}{(\ell-1)-(qb-1)+k} \binom{qb-1}{k} \\ &= \sum_{k=\ell-qb}^{\ell-1} \binom{pa}{k} \binom{qb-1}{(qb-1)-(\ell-1)+k} \end{aligned}$$

V, 20

$$\begin{aligned} \binom{pa+qb-1}{\ell-1} &= \sum_{k=\ell-qb}^{\ell-1} \binom{pa}{k} \binom{qb-1}{\ell-1-k} \\ &= \sum_{k=1}^{\ell-1} \binom{pa}{k} \binom{qb-1}{\ell-1-k} = \sum_{k=1}^{\ell-1} \binom{pa}{k} \binom{qb}{\ell-k} \frac{\ell-k}{qb} \\ &\quad = -\frac{1}{qb} \sum_{k=1}^{\ell-1} \binom{pa}{k} \binom{qb}{\ell-k} k \text{ mod. } \ell. \end{aligned}$$

Damit wird

$$\begin{aligned} L(a,b) &\equiv -\sum_{p,q} \frac{1}{pq} \sum_{k=1}^{\ell-1} \binom{pa}{k} \binom{qb}{\ell-k} k \mod \ell \\ &\equiv -\sum_{k=1}^{\ell-1} k \sum_{p} \frac{1}{p} \binom{pa}{k} \sum_{q} \frac{1}{q} \binom{qb}{\ell-k} \mod \ell. \end{aligned}$$

Wegen $1 \leqq pa \leqq \ell - 1$, $1 \leqq qb \leqq \ell - 1$ gilt nun für $1 \leqq k \leqq \ell - 1$

$$\begin{aligned} \frac{1}{\ell} S_1(\zeta_1^{-k} \lambda_1^{pa}) &= \sum_{\mu \equiv k\,(\ell)}^{0\ldots\ell-1} (-1)^{\mu} \binom{pa}{\mu} = (-1)^k \binom{pa}{k} \\ \frac{1}{\ell} S_1(\zeta_1^{k} \lambda_1^{qb}) &= \sum_{\nu \equiv -k\,(\ell)}^{0\ldots\ell-1} (-1)^{\nu} \binom{qb}{\nu} = (-1)^{\ell-k} \binom{qb}{\ell-k}. \end{aligned}$$

Folglich wird

$$\begin{aligned} L(a,b) &\equiv \sum_{k=1}^{\ell-1} k \cdot \sum_{p} \frac{1}{\ell} S_1 \left(\frac{\zeta_1^{-k} \lambda_1^{pa}}{p} \right) \cdot \sum_{q} \frac{1}{\ell} S_1 \left(\frac{\zeta_1^{k} \lambda_1^{qb}}{q} \right) \mod \ell \\ &\equiv \sum_{k=1}^{\ell-1} k \cdot \frac{1}{\ell} S_1 \left(\zeta_1^{-k} \sum_{p} \frac{\lambda_1^{pa}}{p} \right) \cdot \frac{1}{\ell} S_1 \left(\zeta_1^{k} \sum_{q} \frac{\lambda_1^{qb}}{q} \right) \mod \ell \end{aligned}$$

Da nun wegen $a > 1$ und $b > 1$ die Spuren von Gliedern mit $pa \geqq \ell$ oder $qb \geqq \ell$ durchweg herausfallen, kann die Summation über *alle* positiven p, q erstreckt werden. Das gibt aber

$$L(a,b) \equiv \sum_{k=1}^{\ell-1} k \cdot \frac{1}{\ell} S_1 \left(\zeta_1^{-k} \log \eta_a \right) \cdot \frac{1}{\ell} S_1 \left(\zeta_1^{k} \log \eta_b \right) \mod \ell,$$

V, 21 also meine frühere Formel.

Für *beliebiges* n kann man die störenden p', q' ebenfalls loswerden, nach ganz ähnlichem Muster, wie a. S. 17] für $n = 1$.

1.) a und b prim zu ℓ.

Dann sind in der Formel a. S. 15] unten p und q prim zu ℓ. Ist ferner $pa + qb$ genau durch ℓ^{ϱ} teilbar, so kommt es im Exponenten nur auf $p'a + q'b \mod \ell^{\varrho}$

an. Wie a. S. 17] folgt daraus

$$(\eta_a, \eta_b) = \zeta_n^{-\sum_{p,q} \frac{b}{p} \cdot \frac{1}{pa+qb} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \mu \binom{pa+qb}{\mu}}$$

oder

$$(\eta_a, \eta_b) = \zeta_n^{+\sum_{p,q} \frac{a}{q} \cdot \frac{1}{pa+qb} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \mu \binom{pa+qb}{\mu}}$$

und noch etwas einfacher:

$$\left.\begin{aligned} &(\eta_a, \eta_b) = \zeta_n^{-\sum_{p,q} \frac{b}{p} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \binom{pa+qb-1}{\mu-1}} \\ \text{oder}\quad & \\ &(\eta_a, \eta_b) = \zeta_n^{+\sum_{p,q} \frac{a}{q} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \binom{pa+qb-1}{\mu-1}} \end{aligned}\right\} \text{wenn } a \text{ und } b \text{ prim zu } \ell \text{ sind,}$$

summiert über alle positiven p, q mit

$(p, q, \ell) = 1$ (nicht entbehrlich)
$pa + qb \equiv 0 \bmod. \ell$ (jetzt nicht entbehrlich)
$\ell^n \leqq pa + qb \leqq n\ell^n - (n-1)\ell^{n-1}$ (entbehrlich).

Außer dem Fall 1.) interessiert für die beabsichtigte Anwendung nur noch der folgende Fall 2.): V, 22

2.) a prim zu ℓ, $b = \ell^n$.

Dann ist jedenfalls q prim zu ℓ, weil sicher $p \equiv 0 \bmod. \ell$ ist. Also überträgt sich jedenfalls die zweite der obigen Fassungen:

$$(\eta_a, \eta_{\ell^n}) = \zeta_n^{+\sum_{p,q} \frac{a}{q} \sum_{\mu \equiv 0\,(\ell^n)} (-1)^\mu \binom{pq+q\ell^n-1}{\mu-1}} \quad \text{wenn } a \text{ prim zu } \ell \text{ ist,}$$

summiert über alle positiven p, q mit

$(q, \ell) = 1$ (nicht entbehrlich)
$p \equiv 0 \bmod. \ell$ (jetzt nicht entbehrlich)
$\ell^n \leqq pa + q\ell^n \leqq n\ell^n - (n-1)\ell^{n-1}$ (entbehrlich).

Ich gebe jetzt *für beliebiges* n im Falle

a und b prim zu ℓ

die entsprechende Umformung, wie oben für $n = 1$. Dazu bemerke ich zunächst, daß in der Formel a. S. 21] die Summationsbeschränkung $pa + qb \equiv 0 \bmod. \ell$ nebst $(p, q, \ell) = 1$ ersetzt werden kann durch die einfachere $(p, \ell) = 1$, $(q, \ell) = 1$, wobei zwar überflüssige Glieder hineinkommen, aber nunmehr p und q *unabhängig* von einander laufen, denn unsere Umformung klappt wegen $(p, \ell) = 1$, und die Glieder mit $pa + qb \not\equiv 0 \bmod. \ell$, wo $(p, \ell) = 1$ ist fallen identisch heraus. (Die Einschränkung $(q, \ell) = 1$, die nur aus Symmetriegründen und im Interesse des späteren mitgeführt wird, ist vorläufig sogar entbehrlich). Wir haben also

$$(\eta_a, \eta_b) = \zeta_n^{L(a,b)} \quad \text{mit}$$

$$L(a,b) \equiv -\sum_{(p,\ell)=1}^{1\ldots\infty} \sum_{(q,\ell)=1}^{1\ldots\infty} \frac{b}{p} \sum_{\mu\equiv 0\,(\ell^n)} (-1)^\mu \binom{pa+qb-1}{\mu-1} \bmod. \ell^n.$$

V, 23 Nun ist

$$\binom{pa+qb-1}{\mu-1} = \sum_k \binom{pa}{k} \binom{qb-1}{\mu-1-k},$$

wo die Summation über k von $-\infty$ bis $+\infty$ erstreckt werden darf. Diese Formel folgt unmittelbar aus der Identität

$$(1+x)^{pa+qb-1} = (1+x)^{pa}(1+x)^{qb-1}$$

durch Binomialentwicklung beiderseits. So ergibt sich

$$L(a,b) \equiv -\sum_{(p,\ell)=1}^{1\ldots\infty} \frac{1}{p} \sum_{(q,\ell)=1}^{1\ldots\infty} b \sum_{\mu\equiv 0\,(\ell^n)} \sum_k (-1)^k \binom{pa}{k} (-1)^{\mu-k} \binom{qb-1}{\mu-1-k} \bmod. \ell^n$$

$$\equiv -\sum_{(p,\ell)=1}^{1\ldots\infty} \frac{1}{p} \sum_{(q,\ell)=1}^{1\ldots\infty} \frac{1}{q} \sum_{\mu\equiv 0\,(\ell^n)} \sum_k (-1)^k \binom{pa}{k} (-1)^{\mu-k} \binom{qb}{\mu-k} (\mu-k) \bmod. \ell^n,$$

auch für das Glied mit $\mu - k = 0$, weil $\binom{qb-1}{\mu-1-k}$ dann auch 0 ist. Weiter können wegen $(p, \ell) = 1$, $(q, \ell) = 1$ alle Multipla von ℓ^n fortgelassen werden, also

zunächst der Faktor μ, ferner k durch mod. ℓ^n kongruente ersetzt werden. Das ergibt

$$L(a,b) \equiv \sum_{k=0}^{\ell^n-1} k \sum_{(p,\ell)=1}^{1\ldots\infty} \frac{1}{p} \sum_{\nu\equiv k\,(\ell^n)} (-1)^\nu \binom{pa}{\nu} \cdot$$
$$\cdot \sum_{(q,\ell)=1}^{1\ldots\infty} \frac{1}{q} \sum_{\mu\equiv -k\,(\ell^n)} (-1)^\mu \binom{qb}{\mu} \text{ mod. } \ell^n.$$

Nun ist

$$\sum_{\nu\equiv k\,(\ell^n)} (-1)^\nu \binom{pa}{\nu} = \frac{1}{\ell^n} \mathsf{S}\left(\zeta_n^{-k}\lambda_n^{pa}\right),$$

wo S die Summe über alle ζ_n^i $(i = 0, \ldots, \ell^n - 1)$ bedeutet. Also wird

$$L(a,b) \equiv \sum_{k=0}^{\ell^n-1} k \cdot \frac{1}{\ell^n}\mathsf{S}\left(\zeta_n^{-k} \sum_{(p,\ell)=1}^{1\ldots\infty} \frac{\lambda_n^{pa}}{p}\right) \cdot \frac{1}{\ell^n}\mathsf{S}\left(\zeta_n^{k} \sum_{(q,\ell)=1}^{1\ldots\infty} \frac{\lambda_n^{qb}}{q}\right) \text{ mod. } \ell^n$$
$$\equiv \sum_{k=0}^{\ell^n-1} k \cdot \frac{1}{\ell^n}\mathsf{S}\left(\zeta_n^{-k}\left[\log(1-\lambda_n^a) - \frac{1}{\ell}\log(1-\lambda_n^{a\ell})\right]\right) \cdot$$
$$\cdot \frac{1}{\ell^n}\mathsf{S}\left(\zeta_n^{k}\left[\log(1-\lambda_n^b) - \frac{1}{\ell}\log(1-\lambda_n^{b\ell})\right]\right) \text{ mod. } \ell^n.$$

Schließlich gehe ich noch zu den Basiselementen

$$\tau_a = \prod_{(m,\ell)=1}^{1\ldots\infty} \eta_{am}^{\frac{\mu(m)}{m}}$$

über. Für sie wird V, 24

$$(\tau_a, \tau_b) = \prod_{(m,\ell)=1}^{1\ldots\infty} \prod_{(j,\ell)=1}^{1\ldots\infty} (\eta_{ma}, \eta_{jb})^{\frac{\mu(m)}{m}\,\frac{\mu(j)}{j}}.$$

Nun ist

$$\sum_{(m,\ell)=1}^{1\ldots\infty} \frac{\mu(m)}{m} \sum_{(p,\ell)=1}^{1\ldots\infty} \frac{\lambda_n^{pa}}{p} = \sum_{(P,\ell)=1}^{1\ldots\infty} \frac{\lambda_n^{Pa}}{P} \sum_{m|P} \mu(m) = \lambda_n^a.$$

so folgt

$$(\tau_a, \tau_b) = \zeta_n^{\sum_{k=0}^{\ell^n - 1} k \cdot \frac{1}{\ell^n} \mathsf{S}(\zeta_n^{-k} \lambda_n^a) \cdot \frac{1}{\ell^n} \mathsf{S}(\zeta_n^k \lambda_n^b)} \quad \text{für zu } \ell \text{ prime } a, b.$$

5.3 Lösung der Knoppschen Aufgabe. (28.10.1927)

Solution of a diophantine problem which Hasse had heard from Knopp on the DMV-meeting in Kissingen in September; see the entry of September 28, 1927]. *The problem is due to Kellogg* [Kel21]. *Hasse copies the solution given by Curtiss* [Cur22].

V, 25

(Nach Curtiss, l. c. Tagebuch IV, S. 61])

(28. X. 27).

Unter einer *n–Folge* $\mathfrak{x}_n = (x_1, \ldots, x_n)$ sei eine Folge natürlicher Zahlen verstanden, für die

$$f_n(\mathfrak{x}_n) = \frac{1}{1 - \left(\frac{1}{x_1} + \cdots + \frac{1}{x_n}\right)}$$

endlich und positiv ist. Die Glieder einer n–Folge sind sämtlich $\geqq 2$, und wenn $n \geqq 2$ ist, ist höchstens ein Glied $= 2$.

Die zu beweisende Behauptung lautet dann:

Der Ausdruck $f_n(\mathfrak{x}_n)$ besitzt im Bereich aller n–Folgen $\mathfrak{x}_n$ ein Maximum. Dies wird einzig und allein für diejenige n–Folge $\mathfrak{x}_n = \mathfrak{k}_n$ angenommen, die durch die Rekursionsformeln

$$k_1 - 1 = 1, \quad k_{\nu+1} - 1 = (k_\nu - 1)k_\nu \quad (\nu = 1, \ldots, n-1)$$

definiert wird, und hat den Wert

$$k_{n+1} - 1 = (k_n - 1)k_n.$$

V, 26

Satz 1. $\mathfrak{k}_n$ *ist eine n–Folge mit* $f_n(\mathfrak{k}_n) = k_{n+1} - 1$.

Beweis: Für $n = 1$ ist das richtig. Sei es für $n - 1$ schon bewiesen. Dann ist

$$\frac{1}{f_n(\mathfrak{k}_n)} = \frac{1}{f_{n-1}(\mathfrak{k}_{n-1})} - \frac{1}{k_n} = \frac{1}{k_n - 1} - \frac{1}{k_n} = \frac{1}{(k_n - 1)k_n} = \frac{1}{k_{n+1} - 1}$$

Für $n = 1$ ist die zu beweisende Behauptung ersichtlich richtig, da $f_1(\mathfrak{x}_1) = \frac{1}{1-\frac{1}{x_1}}$ im Bereich aller 1–Folgen $\mathfrak{x}_1 = (x_1)$, d. h. aller natürlichen Zahlen $x_1 \geqq 2$ das Maximum $2 = k_2 - 1$ hat, das einzig und allein für die 1–Folge $\mathfrak{x}_1 = \mathfrak{k}_1 = (k_1) = (2)$ angenommen wird. Ich setze daher im folgenden durchweg $n \geqq 2$ voraus.

Ich nenne dann eine nach steigender Größe geordnete n–Folge $\bar{\mathfrak{x}}_n = (\bar{x}_1, \ldots, \bar{x}_n)$ *reduziert*, wenn

$$(1.) \quad \bar{x}_1 \leqq \bar{x}_2 \leqq \cdots \leqq \bar{x}_{n-1} < \bar{x}_n$$

$$(2.) \quad \bar{x}_n = \big[f_{n-1}(\bar{\mathfrak{x}}_{n-1})\big] + 1$$

ist. Dabei bedeutet hier und im folgenden $\bar{\mathfrak{x}}_{n-1} = (\bar{x}_1, \ldots, \bar{x}_{n-1})$ den $(n-1)$–gliedrigen Anfangsabschnitt von $\overline{\mathfrak{X}}_n$, der ersichtlich (unabhängig von (1.), (2.)) eine $(n-1)$–Folge ist.

V, 27

Satz 2. *Zu jeder n–Folge $\mathfrak{x}_n$ existiert eine reduzierte n–Folge $\bar{\mathfrak{x}}_n$ derart, daß*

$$\mathfrak{x}_n = \bar{\mathfrak{x}}_n\,, \quad f_n(\mathfrak{x}_n) = f_n(\bar{\mathfrak{x}}_n), \quad \textit{wenn } \mathfrak{x}_n \textit{ reduziert,}$$
$$\mathfrak{x}_n \neq \bar{\mathfrak{x}}_n\,, \quad f_n(\mathfrak{x}_n) < f_n(\bar{\mathfrak{x}}_n), \quad \textit{wenn } \mathfrak{x}_n \textit{ nicht reduziert.}$$

Beweis: Es sei $\mathfrak{x}_n$ nicht reduziert*). Dann ist entweder (2.) nicht erfüllt oder (1.) nicht erfüllt.

Ist (2.) nicht erfüllt, so ist auch

$$\mathfrak{x}'_n = (x_1, \ldots, x_{n-1}, x_n - 1)$$

eine (nicht notwendig nach steigender Größe geordnete) n–Folge mit

$$f_n(\mathfrak{x}_n) < f_n(\mathfrak{x}'_n).$$

Nach Definition der n–Folgen ist nämlich

$$\frac{1}{f_n(\mathfrak{x}_n)} = \frac{1}{f_{n-1}(\mathfrak{x}_{n-1})} - \frac{1}{x_n} > 0\,, \quad \text{also} \quad f_{n-1}(\mathfrak{x}_{n-1}) < x_n,$$

d. h. auch

$$[f_{n-1}(\mathfrak{x}_{n-1})] < x_n.$$

*) Alle vorkommenden n–Folgen seien, wo nichts anderes bemerkt ist, nach steigender Größe geordnet vorausgesetzt.

Wenn nun (2.) nicht erfüllt ist, ist sogar

$$[f_{n-1}(\mathfrak{x}_{n-1})] < x_n - 1,$$

also auch

$$f_{n-1}(\mathfrak{x}_{n-1}) < x_n - 1,$$

d. h.

$$\frac{1}{f_n(\mathfrak{x}'_n)} = \frac{1}{f_{n-1}(\mathfrak{x}_{n-1})} - \frac{1}{x_n - 1} > 0,$$

also $\mathfrak{x}'_n$ eine n–Folge, und V, 28

$$\frac{1}{f_n(\mathfrak{x}'_n)} = \frac{1}{f_{n-1}(\mathfrak{x}_{n-1})} - \frac{1}{x_n - 1} < \frac{1}{f_{n-1}(\mathfrak{x}_{n-1})} - \frac{1}{x_n} = \frac{1}{f_n(\mathfrak{x}_n)},$$

also $f_n(\mathfrak{x}_n) < f_n(\mathfrak{x}'_n)$.

Ist auch für $\mathfrak{x}'_n$ (2.) noch nicht erfüllt, so erhält man durch Verkleinerung eines größten Gliedes von $\mathfrak{x}'_n$ um 1 eine neue n–Folge $\mathfrak{x}''_n$ mit $f_n(\mathfrak{x}'_n) < f_n(\mathfrak{x}''_n)$, u. s. f. Nach endlich vielen Schritten muß hierbei eine (2.) genügende n–Folge erreicht werden, da bei jedem Schritt die stets positive Summe aller Folgenglieder um 1 verkleinert wird.

Ich bezeichne die von $\mathfrak{x}_n$ zu dieser (2.) genügenden n–Folge führende Operation mit V. Durch V entsteht also aus einer (2.) nicht genügenden n–Folge $\mathfrak{x}_n$ eine (2.) genügende n–Folge $V\mathfrak{x}_n$ mit

$$f_n(\mathfrak{x}_n) < f_n(V\mathfrak{x}_n).$$

Ist (1.) nicht erfüllt, so sei unter der Operation D der Übergang zu

$$D\mathfrak{x}_n = (2, 2x_1, \ldots, 2x_{n-2}, x_{n-1})$$

verstanden. Das ist wieder eine (nicht notwendig nach steigender Größe geordnete) n–Folge mit

$$f_n(\mathfrak{x}_n) < f_n(D\mathfrak{x}_n).$$

Denn wenn (1.) nicht erfüllt ist, ist $x_{n-1} = x_n$, also

$$\begin{aligned}\frac{1}{f_n(D\mathfrak{x}_n)} &= 1 - \left(\frac{1}{2} + \frac{1}{2x_1} + \cdots + \frac{1}{2x_n}\right) = \frac{1}{2} - \frac{1}{2}\left(\frac{1}{x_1} + \cdots + \frac{1}{x_n}\right) \\ &= \frac{1}{2} - \frac{1}{2}\left(1 - \frac{1}{f_n(\mathfrak{x}_n)}\right) = \frac{1}{2} \cdot \frac{1}{f_n(\mathfrak{x}_n)},\end{aligned}$$

also

$$f_n(\mathfrak{x}_n) = \frac{1}{2} \cdot f_n(D\mathfrak{x}_n).$$

V, 29

Falls (2.) erfüllt ist, möge V, und falls (1.) erfüllt ist, möge D die Identität bedeuten.

Auf die nicht reduzierte n–Folge $\mathfrak{x}_n$ mögen nun abwechselnd die Operationen V und D angewandt werden, d. h. sukzessive die n–Folgen $V\mathfrak{x}_n$, $DV\mathfrak{x}_n$, $VDV\mathfrak{x}_n, \ldots$ gebildet werden, wobei natürlich vor der Anwendung einer neuen Operation stets nach steigender Größe zu ordnen ist. Dies Verfahren werde so lange fortgesetzt, bis eine reduzierte n–Folge $\bar{\mathfrak{x}}_n$ entstanden ist. Ich zeige, daß dies nach endlich vielen Schritten wirklich eintritt, d. h. daß $(VD)^N V\mathfrak{x}_n$ für hinreichend großes N reduziert ist. Dazu beweise ich durch Induktion, daß die

ersten N Glieder von $(VD)^N V\mathfrak{x}_n$ die N ersten Potenzen von 2 sind:

$$(VD)^N V\mathfrak{x}_n = (2, 2^2, \ldots, 2^N; \ldots),$$

wenn $(VD)^{N-1} V\mathfrak{x}_n$ noch nicht reduziert ist.

Für $N = 1$ ist das richtig. Denn ist $V\mathfrak{x}_n$ noch nicht reduziert, so beginnt nach obigem $DV\mathfrak{x}_n$ mit 2, und folglich auch $VDV\mathfrak{x}_n$, weil ja alle Glieder einer n–Folge $\geqq 2$ sind.

Sei es schon für $N - 1$ bewiesen und $(VD)^{N-1} V\mathfrak{x}_n$ noch nicht reduziert.

V, 30

Dann ist also

$$(VD)^{N-1} V\mathfrak{x}_n = (2, 2^2, \ldots, 2^{N-1}; \ldots)$$

und für diese n–Folge ist (1.) nicht erfüllt. Die auf 2^{N-1} folgenden Glieder sind, da $\left(\frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^{N-1}}\right) + \frac{1}{2^{N-1}} = 1$ ist, $> 2^{N-1}$ (sonst keine n–Folge), also mindestens in der Anzahl 2 vorhanden, d. h. $N - 1 \leqq n - 2$ (weil (1.) nicht erfüllt), und

$$(VD)^{N-1} V\mathfrak{x}_n = (2, 2^2, \ldots, 2^{N-1}; X_N, \ldots, X_{n-1}, X_{n-1}).$$

Es ist dann

$$D(VD)^{N-1} V\mathfrak{x}_n = (2, 2^2, \ldots, 2^N; 2X_N, \ldots, 2X_{n-2}; X_{n-1})$$

(nicht notwendig nach steigender Größe geordnet). Da dies n–Folge ist, sind alle auf 2^N folgenden Glieder $> 2^N$ (wie oben), sodaß das größte Glied unter den $n - N$ letzten vorkommt, und dies muß aus demselben Grunde bei jedem der Einzelschritte von V so bleiben, sodaß in der Tat auch

$$VD(VD)^{N-1} V\mathfrak{x}_n = (VD)^N V\mathfrak{x}_n = (2, 2^2, \ldots, 2^N; \ldots)$$

ist. V, 31

Hiernach ist entweder $(VD)^N V\mathfrak{x}_n$ schon für ein $N \leqq n-2$ reduziert, oder das ist nicht der Fall und dann

$$\begin{aligned}(VD)^{n-2}V\mathfrak{x}_n &= (2, 2^2, \dots, 2^{n-2}; X_{n-1}, X_{n-1})\\ D(VD)^{n-2}V\mathfrak{x}_n &= (2, 2^2, \dots, 2^{n-1}; X_{n-1})\\ (VD)^{n-1}V\mathfrak{x}_n &= (2, 2^2, \dots, 2^{n-1}, 2^{n-1}+1),\end{aligned}$$

also $(VD)^{n-1}V\mathfrak{x}_n$ auf alle Fälle reduziert.

Da bei jeder Operation V oder D f_n vergrößert wird, wenn sie nicht die Identität bedeutet, und da für nicht reduziertes $\mathfrak{x}_n$ mindestens eine der sukzessiven Operationen nicht identisch ist, ist damit die Behauptung bewiesen.

Für eine $(n-1)$–Folge $\mathfrak{x}_{n-1} = (x_1, \dots, x_{n-1})$ werde

$$\varphi_{n-1}(\mathfrak{x}_{n-1}) = x_1 \dots x_{n-1}\big(f_{n-1}(\mathfrak{x}_{n-1}) + 1\big)$$

gesetzt.

Satz 3. *Für eine reduzierte n–Folge $\overline{\mathfrak{x}}_n$ gilt*

(3.) $$\overline{x}_1 \leqq \overline{x}_2 \leqq \dots \leqq \overline{x}_{n-1} \leqq f_{n-1}(\overline{\mathfrak{x}}_{n-1})$$

(4.) $$f_n(\overline{\mathfrak{x}}_n) \leqq \varphi_{n-1}(\overline{\mathfrak{x}}_{n-1}).$$

Beweis: a.) Nach (1.) ist

$$\overline{x}_{n-1} < \overline{x}_n\,,$$

und nach (2.) ist

$$\overline{x}_n = [f_{n-1}(\overline{\mathfrak{x}}_{n-1})] + 1.$$

Zusammen ergibt das

$$\overline{x}_{n-1} \leqq [f_{n-1}(\overline{\mathfrak{x}}_{n-1})] \leqq f_{n-1}(\overline{\mathfrak{X}}_{n-1}),$$

also (3.). b.) Weil $\frac{1}{f_n(\overline{\mathfrak{x}}_n)}$ als Bruch mit dem Nenner $\overline{x}_1 \dots \overline{x}_n$ und positiv ganzzahligem Zähler geschrieben werden kann, ist V, 32

$$f_n(\overline{\mathfrak{x}}_n) \leqq \overline{x}_1 \dots \overline{x}_n\,,$$

und folglich nach (2.)

$$f_n(\overline{\mathfrak{x}}_n) \leqq \overline{x}_1 \dots \overline{x}_{n-1}\big([f_{n-1}(\overline{\mathfrak{x}}_{n-1})] + 1\big) \leqq \varphi_{n-1}(\overline{\mathfrak{x}}_{n-1}),$$

also (4.).

Bemerkung: Durch Satz 2 und 3 wird eine obere Abschätzung von $f_n(\mathfrak{x}_n)$ gegeben die nur von der $(n-1)$–Folge $\bar{\mathfrak{x}}_{n-1}$ abhängt, die zu der nach Satz 2 zur n–Folge $\mathfrak{x}_n$ gehörigen reduzierten n–Folge $\bar{\mathfrak{x}}_n$ gehört. Die $(n-1)$–Folge $\bar{\mathfrak{x}}_{n-1}$ braucht natürlich nicht reduziert zu sein. Das folgende kommt nur für $n \geqq 3$ in Frage.

Satz 4. *Zu jeder* (3.) *genügenden* $(n-1)$*–Folge* $\bar{\mathfrak{x}}_{n-1}$ *existiert eine* (3.) *genügende reduzierte* $(n-1)$*–Folge* $\bar{\bar{\mathfrak{x}}}_{n-1}$ *derart, daß*

$$\begin{aligned} &\bar{\mathfrak{x}}_{n-1} = \bar{\bar{\mathfrak{x}}}_{n-1}\,, \quad \varphi_{n-1}(\bar{\mathfrak{x}}_{n-1}) = \varphi_{n-1}(\bar{\bar{\mathfrak{x}}}_{n-1}), \quad \textit{wenn } \bar{\mathfrak{x}}_{n-1} \textit{ reduziert,} \\ &\bar{\mathfrak{x}}_{n-1} \neq \bar{\bar{\mathfrak{x}}}_{n-1}\,, \quad \varphi_{n-1}(\bar{\mathfrak{x}}_{n-1}) < \varphi_{n-1}(\bar{\bar{\mathfrak{x}}}_{n-1}), \quad \textit{wenn } \bar{\mathfrak{x}}_{n-1} \textit{ nicht reduziert.} \end{aligned}$$

Beweis: Es sei $\bar{\mathfrak{x}}_{n-1}$ nicht reduziert, also dafür (1.) oder (2.) nicht erfüllt. Ist (2.) nicht erfüllt, so sei die Operation V wie im Beweis zu Satz 2 erklärt.

V, 33

Ist (1.) nicht erfüllt, so sei unter der Operation H der Übergang zu

$$H\bar{\mathfrak{x}}_{n-1} = \begin{cases} \left(\bar{x}_1, \dots, \bar{x}_{n-3}, \frac{\bar{x}_{n-2}}{2}+1, \frac{\bar{x}_{n-2}}{2}\left(\frac{\bar{x}_{n-2}}{2}+1\right)\right) & \text{für} \quad \bar{x}_{n-2} \equiv 0\ (2) \\ \left(\bar{x}_1, \dots, \bar{x}_{n-3}, \frac{\bar{x}_{n-2}+1}{2}, \bar{x}_{n-2}\frac{\bar{x}_{n-2}+1}{2}\right) & \text{für} \quad \bar{x}_{n-2} \equiv 1\ (2) \end{cases}$$

verstanden. Das ist wieder eine (nicht notwendig nach steigender Größe geordnete) $(n-1)$–Folge mit

$$f_{n-1}(\bar{\mathfrak{x}}_{n-1}) = f_{n-1}(H\bar{\mathfrak{x}}_{n-1}).$$

Denn es ist wegen $\bar{x}_{n-2} = \bar{x}_{n-1}$

$$\begin{aligned} \frac{1}{\bar{x}_{n-2}} + \frac{1}{\bar{x}_{n-1}} &= \frac{2}{\bar{x}_{n-2}} \\ &= \left\{ \begin{array}{l} \frac{1}{\frac{\bar{x}_{n-2}}{2}+1} + \frac{1}{\frac{\bar{x}_{n-2}}{2}\left(\frac{\bar{x}_{n-2}}{2}+1\right)} \\ \frac{1}{\frac{\bar{x}_{n-2}+1}{2}} + \frac{1}{\bar{x}_{n-2}\frac{\bar{x}_{n-2}+1}{2}} \end{array} \right\}. \end{aligned}$$

Falls (2.) erfüllt, möge V, und falls (1.) erfüllt, möge H wieder die Identität bedeuten.

Auf die nicht reduzierte $(n-1)$–Folge $\bar{\mathfrak{x}}_{n-1}$ mögen nun abwechselnd V und H angewandt werden, d. h. sukzessive die $(n-1)$–Folgen $V\bar{\mathfrak{x}}_{n-1}$, $HV\bar{\mathfrak{x}}_{n-1}$,

$VHV\bar{\mathfrak{x}}_{n-1}, \ldots$ gebildet werden, wobei natürlich wieder jedesmal vor der Anwendung einer neuen Operation nach steigender Größe geordnet wird. Dies Verfahren werde fortgesetzt, bis eine reduzierte $(n-1)$–Folge $\bar{\bar{\mathfrak{x}}}_{n-1}$ entstanden ist. Ich zeige, daß dies nach endlich vielen Schritten wirklich eintritt, daß also $(VH)^N V\bar{\mathfrak{x}}_{n-1}$ für hinreichend hohes N reduziert ist, ferner, daß die Bedingung (3.) bei V und H invariant ist, schließlich, daß φ_{n-1} bei V und H, sofern nicht identisch, vergrößert wird. V, 34

Der Endlichkeitsbeweis erledigt sich hier einfach. Ich zeige nämlich, daß $N = 1$ genügt, d. h. daß spätestens $VHV\bar{\mathfrak{x}}_{n-1}$ reduziert ist. Sei nämlich $V\bar{\mathfrak{x}}_{n-1}$ noch nicht reduziert, also

$$V\bar{\mathfrak{x}}_{n-1} = (\overline{X}_1, \ldots, \overline{X}_{n-2}, \overline{X}_{n-2})$$

$$HV\bar{\mathfrak{x}}_{n-1} = \begin{cases} (\overline{X}_1, \ldots, \overline{X}_{n-3}, \frac{\overline{X}_{n-2}}{2} + 1, \frac{\overline{X}_{n-2}}{2}\left(\frac{\overline{X}_{n-2}}{2} + 1\right)) \text{ für } \overline{X}_{n-2} \equiv 0 \ (2) \\ (\overline{X}_1, \ldots, \overline{X}_{n-3}, \frac{\overline{X}_{n-2}+1}{2}, \overline{X}_{n-2}\frac{\overline{X}_{n-2}+1}{2}) \text{ für } \overline{X}_{n-2} \equiv 1 \ (2) \end{cases}$$

(letztere Folgen nicht notwendig nach steigender Größe geordnet). Weil $\overline{X}_{n-2} \geqq 3$ sein muß (sonst $V\bar{\mathfrak{x}}_{n-1}$ keine $(n-1)$–Folge), ist

$$\frac{\overline{X}_{n-2}}{2} + 1 < \overline{X}_{n-2} \quad \text{bezw.} \quad \frac{\overline{X}_{n-2} + 1}{2} < \overline{X}_{n-2}$$

also (nach den Formeln a. S. 33])

$$\frac{\overline{X}_{n-2}}{2}\left(\frac{\overline{X}_{n-2}}{2} + 1\right) > \overline{X}_{n-2} \quad \text{bezw.} \quad \overline{X}_{n-2}\frac{\overline{X}_{n-2} + 1}{2} > \overline{X}_{n-2}\,.$$

Folglich ist das letzte Glied in $HV\bar{\mathfrak{x}}_{n-1}$ das größte, und an ihm beginnt daher die Ausführung der erneuten Operation V, falls $HV\bar{\mathfrak{x}}_{n-1}$ noch nicht reduziert. Falls nun Diese Reduktion des größten Gliedes von $HV\bar{\mathfrak{x}}_{n-1}$ (unter Beibehaltung der übrigen Glieder) bis auf einen Wert $\leqq \overline{X}_{n-2}$ durch V erfolgen würde, so entstünde dabei eine $(n-1)$–Folge (nicht notwendig der Größe nach geordnet), in der jedes Glied $\leqq$ als das entsprechende in $V\bar{\mathfrak{x}}_{n-1}$, das zweitletzte sogar $<$ als das zweitletzte in $V\bar{\mathfrak{x}}_{n-1}$ wäre. Weil aber nach Definition von V das letzte Glied in $V\bar{\mathfrak{x}}_{n-1}$ keiner Verkleinerung mehr fähig ist, ohne die Eigenschaft, $(n-1)$–Folge zu sein, zu zerstören, so zerstört (das letzte Glied ist $\geqq$ als alle anderen) erst recht jede Verkleinerung irgendeines Gliedes oder mehrerer diese Eigenschaft. Denn dabei fällt $\frac{1}{f_{n-1}(V\bar{\mathfrak{x}}_{n-1})}$ ja mindestens um den gleichen Betrag, wie bei Verkleinerung des letzten Gliedes um 1. Somit kann keine $(n-1)$–Folge V, 35

existieren, deren Glieder sämtlich $\leqq$ und eins wirklich $<$ als das entsprechende von $V\mathfrak{x}_{n-1}$ ist, und hiernach muß bei Anwendung von V auf $HV\mathfrak{x}_{n-1}$ die sukzessive Verkleinerung des letzten, größten Gliedes mit einem Wert $> \overline{X}_{n-2}$ enden, der dann nach wie vor der einzige größte in der entstehenden Folge ist.
V, 36 Daher ist V hiermit schon beendet, und liefert eine reduzierte Folge $VHV\mathfrak{x}_{n-1}$.

Zum Nachweis der Invarianz von (3.) bei V und H beweisen wir zunächst, daß (3.) bei V invariant ist. Das ist klar, weil f_{n-1} bei V vergrößert wird (oder jedenfalls nicht verkleinert, falls V identisch), während die Folgenglieder höchstens verkleinert werden. Um ferner zu beweisen, daß (3.) bei H invariant ist, genügt es wegen der schon festgestellten Invarianz von f_{n-1} bei H zu zeigen, daß das größte Glied von $HV\mathfrak{x}_{n-1}$

$$\frac{\overline{X}_{n-2}}{2}\left(\frac{\overline{X}_{n-2}}{2}+1\right) \leqq f_{n-1}(V\mathfrak{x}_{n-1}) \quad \text{bezw.} \quad \overline{X}_{n-2}\frac{\overline{X}_{n-2}+1}{2} \leqq f_{n-1}(V\mathfrak{x}_{n-1})$$

ist. Weil nun $V\mathfrak{x}_{n-1}$ der Bedingung (2.) genügt, ist

$$\overline{X}_{n-2} \leqq f_{n-2}(V\mathfrak{x}_{n-1}) + 1.$$

Nun ist

$$\frac{1}{f_{n-2}(V\mathfrak{x}_{n-1})} - \frac{1}{\overline{X}_{n-2}} = \frac{1}{f_{n-1}(V\mathfrak{x}_{n-1})},$$

also

$$f_{n-2}(V\mathfrak{x}_{n-1}) = \frac{1}{\frac{1}{\overline{X}_{n-2}} + \frac{1}{f_{n-1}(V\mathfrak{x}_{n-1})}},$$

und damit

$$\overline{X}_{n-2} \leqq \frac{1}{\frac{1}{\overline{X}_{n-2}} + \frac{1}{f_{n-1}(V\mathfrak{x}_{n-1})}} + 1,$$

$$1 + \frac{\overline{X}_{n-2}}{f_{n-1}(V\mathfrak{x}_{n-1})} \leqq 1 + \frac{1}{\overline{X}_{n-2}} + \frac{1}{f_{n-1}(V\mathfrak{x}_{n-1})},$$

V, 37

$$\overline{X}^2_{n-2} \leqq f_{n-1}(V\mathfrak{x}_{n-1}) + \overline{X}_{n-2},$$
$$\overline{X}_{n-2}(\overline{X}_{n-2} - 1) \leqq f_{n-1}(V\mathfrak{x}_{n-1}).$$

Es genügt also,

$$\frac{\overline{X}_{n-2}}{2}\left(\frac{\overline{X}_{n-2}}{2}+1\right) \leqq \overline{X}_{n-2}(\overline{X}_{n-2}-1)$$

bezw.

$$\overline{X}_{n-2}\,\frac{\overline{X}_{n-2}+1}{2} \leqq \overline{X}_{n-2}(\overline{X}_{n-2}-1)$$

zu zeigen. Wegen $\overline{X}_{n-2} \geqq 2$ im ersteren, $\overline{X}_{n-2} \geqq 3$ im letzteren Falle ist das aber richtig.

Zum Nachweis, daß φ_{n-1} bei V und H, sofern nicht identisch, vergrößert wird, beweisen wir zunächst, daß φ_{n-1} bei nicht identischem V vergrößert wird. Wir betrachten dazu einen der Schritte von V, der von einer $(n-1)$–Folge

$$\mathfrak{X}_{n-1} = (X_1, \ldots, X_{n-1}),$$

die (2.) nicht genügt und für die (3.) erfüllt ist, zu einer (nicht notwendig nach steigender Größe geordneten) $(n-1)$–Folge

$$\mathfrak{X}'_{n-1} = (X_1, \ldots, X_{n-2}, X_{n-1}-1)$$

führt. Wegen

$$\frac{1}{f_{n-1}(\mathfrak{X}_{n-1})} - \frac{1}{f_{n-1}(\mathfrak{X}'_{n-1})} = \frac{1}{X_{n-1}(X_{n-1}-1)}$$

ist V, 38

$$f_{n-1}(\mathfrak{X}'_{n-1}) = \frac{X_{n-1}(X_{n-1}-1)f_{n-1}(\mathfrak{X}_{n-1})}{X_{n-1}(X_{n-1}-1) - f_{n-1}(\mathfrak{X}_{n-1})}\,.$$

Daraus ergibt sich

$$\begin{aligned}\varphi_{n-1}(\mathfrak{X}'_{n-1}) - \varphi_{n-1}(\mathfrak{X}_{n-1}) &= X_1 \cdots X_{n-2}\Big\{\big(X_{n-1}-1\big)\big(f_{n-1}(\mathfrak{X}'_{n-1})+1\big) \\ &\qquad - X_{n-1}\big(f_{n-1}(\mathfrak{X}_{n-1})+1\big)\Big\} \\ &= X_1 \cdots X_{n-2}\Big\{\frac{X_{n-1}(X_{n-1}-1)^2 f_{n-1}(\mathfrak{X}_{n-1})}{X_{n-1}(X_{n-1}-1) - f_{n-1}(\mathfrak{X}_{n-1})} - \\ &\qquad - X_{n-1}f_{n-1}(\mathfrak{X}_{n-1}) - 1\Big\} \\ &= X_1 \cdots X_{n-2} \\ &\frac{X_{n-1}f_{n-1}^2(\mathfrak{X}_{n-1}) - (X_{n-1}^2 - X_{n-1} - 1)f_{n-1}(\mathfrak{X}_{n-1}) - X_{n-1}(X_{n-1}-1)}{X_{n-1}(X_{n-1}-1) - f_{n-1}(\mathfrak{X}_{n-1})}\,.\end{aligned}$$

Der Nenner dieses Bruches ist positiv, als Nenner des obigen Ausdrucks für $f_{n-1}(\mathfrak{X}'_{n-1})$ mit positivem Zähler. Der Zähler ist quadratisch in $f_{n-1}(\mathfrak{X}_{n-1})$, und seine Ableitung nach $f_{n-1}(\mathfrak{X}_{n-1})$ ist

$$2X_{n-1}f_{n-1}(\mathfrak{X}_{n-1}) - (X_{n-1}^2 - X_{n-1} - 1);$$

diese wird für $f_{n-1}(\mathfrak{X}_{n-1}) = X_{n-1}$ zu

$$X_{n-1}^2 + X_{n-1} + 1 > 0,$$

also auch für alle $f_{n-1}(\mathfrak{X}_{n-1}) \geqq X_{n-1}$, d. h. die quadratische Funktion wächst in diesem Bereich. Da sie für $f_{n-1}(\mathfrak{X}_{n-1}) = X_{n-1}$ den Wert

$$\begin{aligned} X_{n-1}^3 - (X_{n-1}^2 - X_{n-1} - 1)X_{n-1} - (X_{n-1}^2 - X_{n-1}) \\ = 2X_{n-1} > 0 \end{aligned}$$

V, 39 hat, ist sie also für alle $f(\mathfrak{X}_{n-1}) \geqq X_{n-1}$ positiv. Die letztere Tatsache ist aber, weil $\mathfrak{X}_{n-1}$ (3.) genügend angenommen wird, erfüllt, und damit

$$\varphi_{n-1}(\mathfrak{X}'_{n-1}) > \varphi_{n-1}(\mathfrak{X}_{n-1})$$

bewiesen, also auch

$$\varphi_{n-1}(V\mathfrak{X}_{n-1}) > \varphi_{n-1}(\mathfrak{X}_{n-1}),$$

wenn V nicht identisch und $\mathfrak{X}_{n-1}$ (3.) genügt, wie es im benötigten Zusammenhang der Fall ist.

Schließlich zeigen wir, daß φ_{n-1} auch bei nicht identischem H vergrößert wird. Ist an der einzigen Stelle, wo H angewandt wird, H nicht identisch, so ist

$$\begin{aligned} V\overline{\mathfrak{X}}_n &= (\overline{X}_1, \dots, \overline{X}_{n-2}, \overline{X}_{n-2}) \\ HV\overline{\mathfrak{X}}_n &= (\overline{X}_1, \dots, \overline{X}_{n-3}, \frac{\overline{X}_{n-2}}{2} + 1, \frac{\overline{X}_{n-2}}{2}\left(\frac{\overline{X}_{n-2}}{2} + 1\right)) \\ \text{bezw.} \quad & (\overline{X}_1, \dots, \overline{X}_{n-3}, \frac{\overline{X}_{n-2} + 1}{2}, \overline{X}_{n-2}\frac{\overline{X}_{n-2} + 1}{2}). \end{aligned}$$

Wegen der bewiesenen Invarianz von f_{n-2} bei H genügt es zu zeigen, daß

$$\begin{aligned} \overline{X}_{n-2}^2 &< \left(\frac{\overline{X}_{n-2}}{2} + 1\right)^2 \frac{\overline{X}_{n-2}}{2} \\ \text{bzw.} \quad & \left(\frac{\overline{X}_{n-2} + 1}{2}\right)^2 \overline{X}_{n-2} \end{aligned}$$

ist. Nach Wegdivision von $\overline{X}_{n-2}$ führt das auf

$$2\overline{X}_{n-1} < \left(\frac{\overline{X}_{n-1}}{2} + 1\right)^2, \quad \text{d. h.} \quad 0 < \left(\frac{\overline{X}_{n-1}}{2} - 1\right)^2$$

$$\text{bzw.} \quad 4\overline{X}_{n-1} < \left(\overline{X}_{n-2} + 1\right)^2, \quad \text{d. h.} \quad 0 < \left(\overline{X}_{n-2} - 1\right)^2$$

was beides richtig ist, weil $\overline{X}_{n-1}$ wie schon a. S. 34] gesagt, $\geqq 3$ ist. V, 40

Damit ist Satz 4 bewiesen.

Satz 5. *Für eine reduzierte* $(n-1)$*–Folge* $\overline{\overline{\mathfrak{X}}}_{n-1}$ *mit der Eigenschaft* (3.) *gilt*

(5.) $$\overline{\overline{x}}_1 \leqq \overline{\overline{x}}_2 \leqq \cdots \leqq \overline{\overline{x}}_{n-2} \leqq f_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2})$$

(6.) $$\varphi_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) \leqq \varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2})\left(\varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1\right).$$

Beweis: a.) Wie unter a.) im Beweis zu Satz 3 folgt (5.).

b.) Wie im Beweis zu Satz 3 unter b.) ist

$$f_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) \leqq \overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-1},$$

also

$$\begin{aligned}\varphi_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) &= \overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-1}\left(f_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) + 1\right)\\ &\leqq \overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-1}(\overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-1} + 1)\end{aligned}$$

Wegen der Reduziertheit von $\overline{\overline{\mathfrak{X}}}_{n-1}$ ist nun

$$\overline{\overline{x}}_{n-1} = \left[f_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2})\right] + 1 \leqq f_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1,$$

also

$$\begin{aligned}\varphi_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) &\leqq \overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-2}\left(f_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1\right)\cdot\\ &\cdot\left(\overline{\overline{x}}_1 \cdots \overline{\overline{x}}_{n-2}\left(f_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1\right) + 1\right)\\ &= \varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2})\left(\varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1\right),\end{aligned}$$

d. h. (6.).

V, 41

Beweis des Hauptsatzes: Ich wende das mit den Sätzen 2—5 begonnene Verfahren solange an, wie möglich. Sätze 2,3 kommen für $n \geqq 2$ in Frage, Sätze 4,5 für $n \geqq 3, \ldots$ Aus der vorgegebenen n–Folge $\mathfrak{X}_n$ entsteht

dabei eine Serie von $(n-\nu+1)$–Folgen $\overset{\nu}{\mathfrak{X}}_{n-\nu+1}$ $(\nu = 1, \ldots, n-1)$ nebst deren zugehörigen $(n-\nu)$–Folgen $\overset{\nu}{\mathfrak{X}}_{n-\nu}$ (nämlich den ersten $n-\nu$ Gliedern) mit folgenden Eigenschaften

$$\overset{\nu}{\mathfrak{X}}_{n-\nu+1} \quad \text{ist reduziert} \tag{7}$$

(8)
$$\left\{ \begin{aligned} & f_n(\mathfrak{X}_n) \leqq f_n(\mathfrak{X}_n) \leqq \varphi_{n-1}(\overline{\mathfrak{X}}_{n-1}) \\ & \varphi_{n-\nu+1}(\overset{\nu}{\mathfrak{X}}_{n-\nu+1}) \leqq \varphi_{n-\nu+1}(\overset{\nu}{\mathfrak{X}}_{n-\nu+1}) \leqq \varphi_{n-\nu}(\overset{\nu}{\mathfrak{X}}_{n-\nu}) \left(\varphi_{n-\nu}(\overset{\nu}{\mathfrak{X}}_{n-\nu}) + 1 \right) \\ & \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\nu = 2, \ldots, n-1) \end{aligned} \right\}$$

$$\overset{\nu}{x}_1 \leqq \cdots \leqq \overset{\nu}{x}_{n-\nu} \leqq f_{n-\nu}(\overset{\nu}{\mathfrak{X}}_{n-\nu}) \qquad (\nu = 1, \ldots, n-1) \tag{9}$$

(10)
$\left\{ \right.$ Dann und nur dann, wenn $\mathfrak{X}_n$ bzw. $\overset{\nu-1}{\mathfrak{X}}_{n-\nu+1}$ reduziert ist, ist $\mathfrak{X}_n = \overline{\mathfrak{X}}_n$ bzw. $\overset{\nu-1}{\mathfrak{X}}_{n-\nu+1} = \overset{\nu}{\mathfrak{X}}_{n-\nu}$, und dann und nur dann steht in den Relationen (8) an der betr. ersten Stelle das Gleichheitszeichen $\left. \right\}$.

V, 42

Nun ist $\overset{n-1}{\mathfrak{X}}_1 = (\overset{n-1}{x}_1)$ wegen der letzten Bedingung (9) der Relation

$$\overset{n-1}{x}_1 \leqq f_1(\overset{n-1}{\mathfrak{X}}_1) = \frac{1}{1 - \frac{1}{\overset{n-1}{x}_1}},$$

also

$$\overset{n-1}{x}_1 \leqq 2$$

unterworfen, und somit

$$\overset{n-1}{x}_1 = 2.$$

Damit wird

$$\varphi_1(\overset{n-1}{\mathfrak{X}}_1) = \overset{n-1}{x}_1\big(f_1(\overset{n-1}{\mathfrak{X}}_1) + 1\big) = 2 \cdot 3 = k_3 - 1$$

Nach den a. S. 25] angegebenen Rekursionsformeln für die $k_\nu - 1$ und den Formeln (8) wird daher sukzessive

$$\varphi_2(\overset{n-2}{\mathfrak{X}}_2) \leqq \varphi_2(\overset{n-1}{\mathfrak{X}}_2) \leqq \varphi_1(\overset{n-1}{\mathfrak{X}}_1)\big(\varphi_1(\overset{n-1}{\mathfrak{X}}_1) + 1\big) = (k_3 - 1)k_3 = k_4 - 1$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\varphi_{n-1}(\overline{\mathfrak{X}}_{n-1}) \leqq \varphi_{n-1}(\overline{\overline{\mathfrak{X}}}_{n-1}) \leqq \varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2})\big(\varphi_{n-2}(\overline{\overline{\mathfrak{X}}}_{n-2}) + 1\big)$$

$$\leqq k_{n+1} - 1$$

$$f_n(\mathfrak{X}_n) \leqq f_n(\overline{\mathfrak{X}}_n) \leqq \varphi_{n-1}(\overline{\mathfrak{X}}_{n-1}) \leqq k_{n+1} - 1.$$

Damit ist zunächst gezeigt, daß $f_n(\mathfrak{X}_n)$ für jede beliebige n–Folge $\mathfrak{X}_n$ den Wert $k_{n+1} - 1$ nicht übertrifft, daß also $f_n(\mathfrak{X}_n)$ im Bereich aller n–Folgen wirklich ein Maximum besitzt, welches $\leqq k_{n+1} - 1$, und wegen Satz 1 sogar $= k_{n+1} - 1$ ist.

Es bleibt noch der Nachweis, daß dies Maximum nur für die n–Folge $\mathfrak{X}_n = \mathfrak{k}_n$ angenommen wird. Daß $f_n(\mathfrak{k}_n) = k_{n+1} - 1$ ist, wurde bereits in Satz 1 gezeigt. Soll $f(\mathfrak{X}_n) = k_{n+1} - 1$ werden, so ist nach dem Vorhergehenden erforderlich, daß in den Relationen (8) durchweg das Gleichheitszeichen steht. V, 43

Dazu müssen nach (10) neben (7) auch $\mathfrak{X}_n, \overline{\mathfrak{X}}_{n-1}, \ldots, \overset{n-2}{\mathfrak{X}}_2$ reduziert sein $\Big(\overset{n-1}{\mathfrak{X}}_1$ ist nach obigem reduziert, nämlich $= (2)\Big)$, wobei dann gilt V, 44

$$\mathfrak{X}_n = \overline{\mathfrak{X}}_n$$

$$\overline{\mathfrak{X}}_{n-1} = \overline{\overline{\mathfrak{X}}}_{n-1}$$

$$\cdots\cdots\cdots$$

$$\overset{n-2}{\mathfrak{X}}_2 = \overset{n-1}{\mathfrak{X}}_2\,,$$

was einfach besagt, daß jeder Anfangsabschnitt von

$$\mathfrak{X}_n = (x_1, \ldots, x_n)$$

reduziert sein muß. Daraus folgt aber sukzessive

$$\left.\begin{array}{ll} x_1 = 2 & = k_1 \\ x_2 = [f_1(\mathfrak{k}_1)] + 1 & = k_2 \\ x_3 = [f_2(\mathfrak{k}_2)] + 1 & = k_3 \\ \multicolumn{2}{c}{\dotfill} \\ x_n = [f_{n-1}(\mathfrak{k}_{n-1})] + 1 & = k_n \end{array}\right\} \quad \text{also} \quad \mathfrak{X}_n = \mathfrak{k}_n$$

weil ja nach Satz 1 allgemein

$$[f_\nu(\mathfrak{k}_\nu)] = f_\nu(\mathfrak{k}_\nu) = k_{\nu+1} - 1 \qquad (\nu = 1, 2, \ldots, n-1)$$

ist.

Damit ist die Behauptung a. S. 25] vollständig bewiesen.

5.4 Die durch eine primitive quadratische Form darstellbaren Zahlen. (30.12.1927)

Ideal theoretic characterization of those integers which are represented by primitive binary quadratic forms. Nothing is said about the motivation for this investigation. But since the result is used in the next entry] we may assume that the present entry is meant as a preparation for the next, although the result here is also of independent interest.

V, 45

(30. XII. 27)

Ich suche die durch eine primitive quadratische Form $ax^2+bxy+cy^2$ darstellbaren Zahlen m idealtheoretisch zu charakterisieren. Es sei $D = f^2 d = b^2 - 4ac$ die Diskriminante der Form, dabei d die zugehörige Körperdiskriminante und die Form sei ohne Einschränkung positiv–definit vorausgesetzt, falls $D < 0$ ist. Für $D > 0$ sei ferner die Form von vorneherein so transformiert, daß $a > 0$ ist. Auf alle Fälle wird also

$$a > 0$$

vorausgesetzt. Ferner natürlich D als Nichtquadratzahl, insbesondere $D \neq 0$, sodaß d einen Sinn hat und $\neq 1$ ist. Schließlich kann die Form auch noch von vorneherein so transformiert werden, daß

$$(a, f) = 1$$

ist. Ist das nämlich nicht der Fall und sind p, q, r die Primteiler von f und zwar $p \nmid a$, $q|a$ aber $q \nmid c$, $r|a$ und $r|c$ also $r \nmid b$, so bestimme man teilerfremde α, β so, daß

$$\begin{array}{ll} \alpha \equiv 1 \ (p) & \beta \equiv 0 \ (p) \\ \alpha \equiv 0 \ (q) & \beta \equiv 1 \ (q) \\ \alpha \equiv 1 \ (r) & \beta \equiv 1 \ (r). \end{array}$$

Das ist ersichtlich möglich, weil diese unabhängigen Bedingungen auch keinen gemeinsamen Teiler von α, β implizieren. Eine unimodulare Transformation $\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$ führt dann die Form in eine neue mit dem ersten Koeffizienten

$$a\alpha^2 + b\alpha\beta + c\beta^2 \equiv \left\{ \begin{array}{c} a \ (p) \\ c \ (q) \\ b \ (r) \end{array} \right\}, \quad \text{also prim zu } f$$

über. Durch passende Wahl von α, β kann dieser natürlich zudem wieder po-
V, 46 sitiv gemacht werden (α hinreichend groß, zuvor β fest). Durch die genannten Transformationen werden D und die m und die Primitivität nicht geändert, sodaß es keine Einschränkung ist, für die zu lösende Aufgabe diese speziellen Voraussetzungen einzuführen.

Wir betrachten also jetzt eine quadratische Form

$$ax^2 + bxy + cy^2$$

mit den Eigenschaften

$$(a, b, c) = 1, \qquad a > 0, \qquad (a, f) = 1$$

wo

$$D = b^2 - 4ac = f^2 d, \quad d \text{ Körperdiskriminante.}$$

Wir setzen

$$\omega = \frac{d + \sqrt{d}}{2},$$

sodaß der Modul $[1, \omega] = \mathsf{R}$ der Ring aller ganzen Zahlen des zugeordneten quadratischen Körpers ist, und ebenso $[1, f\omega] = \mathsf{R}_f$ der Ring aller mod. f einer rationalen Zahl kongruenten ganzen Körperzahlen.

Es ist

$$ax^2 + bxy + cy^2 = \frac{\left(ax + \frac{b+\sqrt{D}}{2}y\right)\left(ax + \frac{b-\sqrt{D}}{2}y\right)}{a} = \frac{N(\alpha)}{a},$$

wobei

$$\alpha = ax + \frac{b + \sqrt{D}}{2} = ax + \left(\frac{b - fd}{2} + f\omega\right) y$$

ersichtlich eine ganze Körperzahl, sogar eine Zahl aus R_f ist ($fd \equiv f^2 d \equiv b^2 \equiv b \bmod. 2$). Hierbei ist nun der Modul

$$\left[a, \frac{b + \sqrt{D}}{2}\right] = \left[a, \frac{b - fd}{2} + f\omega\right] = \mathfrak{a}_f$$

V, 47 ein Ideal in R_f.Denn die Multiplikation der Basiselemente mit $f\omega$ liefert nach

leichter Rechnung:

$$f\omega \cdot a = -\frac{b-fd}{2} \cdot a + a \cdot \left(\frac{b-fd}{2} + f\omega\right)$$
$$f\omega\left(\frac{b-fd}{2} + f\omega\right) = -c \cdot a + \left(\frac{b-fd}{2} + fd\right) \cdot \left(\frac{b-fd}{2} + f\omega\right).$$

Sei nun

$$\left(a, \frac{b-fd}{2} + f\omega\right) = \mathfrak{a}$$

das zugeordnete Ideal in R, d. h. der größte gemeinsame Teiler der Basiselemente. Nach dem verallgemeinerten Gaussschen Satz folgt dann, weil die quadratische Form primitiv ist,

$$N(\mathfrak{a}) = a$$

Dies $\mathfrak{a}$ hat keinen ganz–rationalen Teiler, weil ein solcher in a und f aufginge. Daher ist $a = N(\mathfrak{a})$ das kleinste ganz–rationale Multiplum von $\mathfrak{a}$.

Hieraus ergibt sich, daß $\mathfrak{a}_f$ der Durchschnitt von $\mathfrak{a}$ mit R_f ist. Einerseits gehört ja nach obigem jedes $\alpha = ax + \left(\frac{b-fd}{2} + f\omega\right) y$ aus $\mathfrak{a}_f$ zu $\mathfrak{a}$ und R_f. Andererseits führt für ein

$$\alpha = r + sf\omega \equiv 0 \text{ mod. } \mathfrak{a}$$

aus $\mathfrak{a}$ und R_f der Ansatz

$$\alpha = r + sf\omega = ax + \left(\frac{b-fd}{2} + f\omega\right) y$$

auf

$$y = s$$
$$ax = r - \frac{b-fd}{2} s,$$

und wegen

$$\frac{b-fd}{2} s \equiv -f\omega s \text{ mod. } \mathfrak{a},$$
$$r \equiv -f\omega s \text{ mod. } \mathfrak{a}$$

ist

$$r - \frac{b - fd}{2} s \equiv 0 \text{ mod. } \mathfrak{a}, \quad \text{also nach obigem mod. } a,$$

V, 48 sodaß wirklich x, y **ganzzahlig** ausfallen, also α zu $\mathfrak{a}_f$ gehört.

Aus dem Vorhergehenden ergibt sich jetzt, daß die Gesamtheit aller

$$m = ax^2 + bxy + cy = \frac{N(\alpha)}{N(\mathfrak{a})}$$

erhalten wird, wenn man α alle zu R_f gehörigen, durch $\mathfrak{a}$ teilbaren Zahlen durchlaufen läßt.

Setzt man noch

$$\mathfrak{a}\mathfrak{c} = \alpha$$

so wird

$$m = \big(\text{sgn.} N(\alpha)\big).N(\mathfrak{c})$$

und $\mathfrak{c}$ durchläuft alle ganzen Ideale, für die $\mathfrak{a}\mathfrak{c} = \alpha$ in R_f liegt, und nur diese.

Daraus ergibt sich, unter Beschränkung auf zu f prime m, was auch α und V, 49 $\mathfrak{c}$ prim zu f bedeutet, folgendes Resultat:

Die ganzzahlig durch eine primitive quadratische Form $ax^2 + bxy + cy^2$ mit $a > 0$ der Diskriminante $D = f^2 d$ darstellbaren zu f primen ganzen positiven Zahlen m sind identisch mit den Idealnormen aus einer Idealklasse nach der Idealgruppe

$$\left\{ \begin{array}{c} \alpha \equiv \text{rat. Zahl. mod. } f \\ N(\alpha) > 0 \end{array} \right\} \quad \text{im Körper der } \sqrt{d},$$

und im Falle $D > 0$ die entsprechenden negativen m mit den negativen Idealnormen aus einer anderen solchen Idealklasse.

5.5 Herleitung des Gauss'schen biquadratischen Reziprozitätsgesetzes (zweiter Ergänzungssatz) aus dem allgemeinen Gesetz. (1.1.1928)

Hasse and Artin had recently composed a joint paper on the so-called 2nd supplement to the reciprocity law for arbitrary prime powers ℓ^n in the field of ℓ^n-th roots of unity [AH28]. *Hasse had sent the manuscript to Artin at the end of November 1927, hence about one month prior to this entry. Here, Hasse discusses that general result in the special case of $\ell^n = 4$ with the aim of obtaining from this the well known Gauss' rational criterion for 2 to be a biquadratic residue modulo a prime number p. Many years later Hasse published a generalization, replacing 4 by an arbitrary power 2^n, and accordingly studying the general symbol $\left(\frac{2}{a}\right)_{2^n}$ in the field of 2^n-th root of unity* [Has58].

V, 50

(1. I. 28)

Satz. *Ist p eine Primzahl $\equiv 1 \bmod. 4$, so ist 2 dann und nur dann biquadratischer Rest* mod. p *(im Körper der rationalen Zahlen), wenn p in der Form $x^2 + 64y^2$ darstellbar ist.*

Beweis: Damit 2 biquadratischer Rest mod. p im Körper der rationalen Zahlen ist, ist notwendig und hinreichend, daß 2 biquadratischer Rest mod. π im Gauss'schen Zahlkörper ist, wo π einer der beiden Primfaktoren 1. Grades von p im Gaussschen Zahlkörper ist. Nach meiner gemeinsamen Arbeit mit Artin (Hamb. Abh. 1928) ist nun dieser biquadratische Charakter

$$\left(\frac{2}{\pi}\right) = \left(\frac{1+i}{\pi}\right)\left(\frac{1-i}{\pi}\right) = \left(\frac{1-i}{\pi'}\right)^{-1}\left(\frac{1-i}{\pi}\right) = \left(\frac{i-1}{\frac{\pi}{\pi'}}\right)$$
$$= i^{\,-\frac{1}{4}S\left(\frac{i}{1-i}\log\frac{\pi}{\pi'}\right)}, \quad \text{wo} \quad \pi\pi' = p$$

Also ist 2 dann und nur biquadratischer Rest mod. p, wenn

$$S\left(\frac{i}{1-i}\log\frac{\pi}{\pi'}\right) \equiv 0 \bmod. 16$$

ist. Nun ist

$$S\left(\frac{i}{1-i}\log\frac{\pi}{\pi'}\right) = \frac{i}{1-i}(\log\pi - \log\pi') - \frac{i}{1+i}(\log\pi - \log\pi')$$
$$= i\left(\frac{1}{1-i} - \frac{1}{1+i}\right)(\log\pi - \log\pi')$$
$$= \log\pi' - \log\pi$$

Folglich ist notwendig und hinreichend

$$\log\pi' \equiv \log\pi \mod 16,$$

V, 51 und das ist gleichbedeutend mit

$$\pi' \equiv i^\nu\pi \mod 16.$$

Hierin muß zunächst ν gerade sein, weil aus $\pi' \equiv \pm i\pi \mod 16$ folgte $\pi + \pi' \equiv (1 \pm i)\pi$ nicht durch 2 teilbar, während noch aus $\pi = x + yi$, $\pi' = x - yi$ folgt, daß $\pi + \pi' = 2x$ ist.

Ich zeige nun, daß die hiernach notwendige und hinreichende Bedingung

$$(1) \qquad \pi' \equiv (-1)^\mu\pi \mod 16$$

gleichbedeutend ist mit der Bedingung

$$(2) \qquad \pi \equiv i^k r \mod 8 \qquad (r \text{ rational}).$$

Einerseits folgt nämlich aus (1) und einer der beiden Relationen

$$\pi + \pi' = 2x$$
$$\pi - \pi' = 2iy,$$

daß

$$2\pi \equiv 2x \mod 16, \quad \pi \equiv x \mod 8 \qquad (\mu = 0)$$
$$2\pi \equiv 2iy \mod 16, \quad \pi \equiv iy \mod 8 \qquad (\mu = 1)$$

ist. Andererseits folgt aus (2)

$$y \equiv 0 \mod 8 \qquad (k = 0, 2)$$
$$x \equiv 0 \mod 8 \qquad (k = 1, 3),$$

was ohne weiteres (1) ergibt. Die Bedingung (2) bedeutet nun die Zugehörigkeit des Hauptideals (π) zum Ring R_8^+ (siehe S. 46]), der hier mit R_8 zusammenfällt. Dieser Ring entspricht nach dem Satz a. S. 49] der Form $x^2 + 64y^2$, sodaß in der Tat $p = x^2 + 64y^2$ notwendige und hinreichende Bedingung ist (was übrigens auch aus dem eben geführten Beweis direkt, ohne Vermittlung der Ringklassentheorie entnommen werden kann). V, 52

5.6 Theorie der Funktion $x^{x^{x^{\cdot^{\cdot^{\cdot}}}}}$ (30.1.1928)

We do not know Hasse's motivation for this entry. Perhaps he wished to hand out this problem to his students, since on one point he refers to his lecture course on analysis. Already Eisenstein, who had studied this function when he was 15 years, had said in his paper [Eis44] *that this would be a good exercise for beginners.*

V, 53

(30. I. 28)

Diese Funktion ist als die Grenzfunktion der Folge

$$f_0(x) = 0, \quad f_1(x) = x^{f_0(x)} = 1, \quad f_2(x) = x^{f_1(x)} = x,$$
$$f_3(x) = x^{f_2(x)} = x^x, \ldots,$$

allgemein

$$f_{n+1}(x) = x^{f_n(x)} \quad (n \geqq 0) \quad \text{nebst} \quad f_0(x) = 0$$

erklärt, wenn eine solche vorhanden. Als Argumente kommen a priori nur $x > 0$ in Frage.

Es gilt nun der

Satz. *Die Grenzfunktion* $y = x^{x^{x^{\cdot^{\cdot^{\cdot}}}}}$ *existiert dann und nur dann, wenn*

$$\left(\tfrac{1}{e}\right)^e \leqq x \leqq e^{\frac{1}{e}}$$

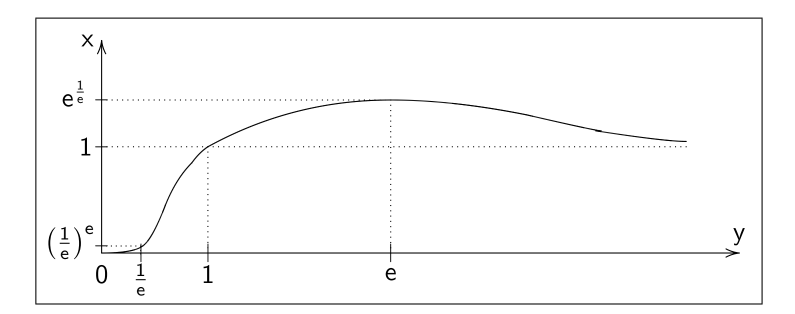
ist, und sie ist dann der durch die Nebenbedingung

$$\tfrac{1}{e} \leqq y \leqq e$$

eindeutig bestimmte inverse Zweig von

$$x = y^{\frac{1}{y}}.$$

Beweis: 1.) Eine elementare Diskussion der Funktion $x = y^{\frac{1}{y}}$ ergibt folgenden Verlauf:



Die Funktion wächst monoton i. e. S. von $0 \ldots e$ und fällt monoton i. e. S. von $e \ldots + \infty$. Dabei

$$\lim_{y \to 0} y^{\frac{1}{y}} = 0, \qquad \lim_{y \to +\infty} y^{\frac{1}{y}} = 1.$$

Bei e hat sie ein Maximum. Bei 1 ist sie gleich 1 mit Steigung 1. Die Wendepunkte ergeben sich als die beiden Lösungen von V, 54

$$1 - \lg y = y + \sqrt{y + y^2}\,, \quad \text{ungefähr} \quad 0{,}58 \ldots 0{,}59 > \frac{1}{e}$$
$$1 - \lg y = y - \sqrt{y + y^2}\,, \quad \text{ungefähr} \quad 4{,}36 \ldots 4{,}37 > e$$

(Siehe dazu Übungen zur Integralrechnung vom 16. XII. 25).

2.) Wenn $y = \lim_{n \to \infty} f_n(x)$ existiert, so folgt

$$y = \lim_{n \to \infty} f_n(x) = \lim_{n \to \infty} x^{f_{n-1}(x)} = x^{\lim_{n \to \infty} f_{n-1}(x)} = x^y,$$

also sicher $y > 0$, weil $y \geqq 0$ und weil $0 = x^0 = 1$ nicht sein kann, und daher

$$x = y^{\frac{1}{y}}.$$

Welchem Zweige der inversen Funktion das angehört, steht zunächst nicht fest. Für $x < 1$ ist natürlich Eindeutigkeit vorhanden, nicht aber für $x \geqq 1$.

3.) Sei $\boldsymbol{x > e^{\frac{1}{e}}}$. Nach 2.), 1.) kann dann kein Grenzwert existieren.

4.) Sei $\boldsymbol{1 \leqq x \leqq e^{\frac{1}{e}}}$. Dann ist die Folge $f_n(x)$ monoton in n. Denn

$$f_0(x) = 0 < f_1(x) = 1$$

und aus

$$f_{n-1}(x) \leqq f_n(x) \qquad (n \geqq 1)$$

folgt wegen $x \geqq 1$

$$f_n(x) = x^{f_{n-1}(x)} \leqq x^{f_n(x)} = f_{n+1}(x).$$

V, 55 Somit existiert ein Grenzwert, aber ev. $+\infty$, $\big($wie z. B. in 3.)$\big)$. Wegen $x \leqq e^{\frac{1}{e}}$ folgt nun aber

$$f_n(x) \leqq e.$$

Denn

$$f_0(x) = 0 < e$$

und aus

$$f_{n-1}(x) \leqq e \qquad (n \geqq 1)$$

folgt

$$f_n(x) = x^{f_{n-1}(x)} \leqq x^e \leqq \left(e^{\frac{1}{e}}\right)^e = e$$

Somit existiert ein endlicher Grenzwert $y \leqq e$. Damit ist zugleich der inverse Zweig, wie im Satz angegeben, festgelegt.

5.) Sei $\boldsymbol{\left(\frac{1}{e}\right)^e \leqq x < 1}$. Dann ist die Folge $f_n(x)$ alternierend in n, nämlich

$$0 = f_0(x) < f_2(x) < \cdots < f_3(x) < f_1(x) = 1$$

Zunächst ist nämlich

$$f_0(x) = 0 < f_1(x) = 1.$$

Aus der Annahme

$$f_{2n}(x) < f_{2n+1}(x) \qquad (n \geqq 0)$$

folgt ferner wegen $x < 1$

$$f_{2n+1}(x) = x^{f_{2n}(x)} > x^{f_{2n+1}(x)} = f_{2n+2}(x)$$

und daraus

$$f_{2n+2}(x) = x^{f_{2n+1}(x)} < x^{f_{2n+2}(x)} = f_{2n+3}(x)$$

also die Allgemeingültigkeit jener Annahme und überdies der Tatsache

$$f_{2n+1}(x) > f_{2n+2}(x) \qquad (n \geqq 0)$$

Um obige Ungleichungen festzustellen ist dann nur noch V, 56

$$f_{2n}(x) < f_{2n+2}(x), \quad f_{2n+3}(x) < f_{2n+1}(x) \qquad (n \geqq 0)$$

zu beweisen. Die erstere ist für $n = 0$ richtig:

$$f_0(x) = 0 < f_2(x) = x.$$

Wird sie für ein $n \geqq 0$ angenommen, so folgt

$$f_{2n+1}(x) = x^{f_{2n}(x)} > x^{f_{2n+2}(x)} = f_{2n+3}(x),$$

also die zweite, und daraus

$$f_{2n+2}(x) = x^{f_{2n+1}(x)} < x^{f_{2n+3}(x)} = f_{2n+4}(x),$$

also die Allgemeingültigkeit beider.

Hiernach existieren

$$y_1 = \lim_{n\to\infty} f_{2n}(x)\,, \quad y_2 = \lim_{n\to\infty} f_{2n+1}(x)$$
$$0 < y_1 \leqq y_2 < 1,$$

und es genügt ihre Gleichheit

$$y_1 = y_2 = y$$

zu beweisen. Nun ist jedenfalls

$$y_1 = \lim_{n\to\infty} f_{2n}(x) = \lim_{n\to\infty} x^{f_{2n-1}(x)} = x^{\lim\limits_{n\to\infty} f_{2n-1}(x)} = x^{y_2}$$
$$y_2 = \lim_{n\to\infty} f_{2n+1}(x) = \lim_{n\to\infty} x^{f_{2n}(x)} = x^{\lim\limits_{n\to\infty} f_{2n}(x)} = x^{y_1},$$

also weiter y_1, y_2 Lösungen von

$$x^{x^u} = u \qquad (0 < u < 1),$$

also auch von

$$x^u \lg x = \lg u\,, \quad \text{d. h.} \quad x^u \lg\frac{1}{x} = \lg\frac{1}{u}\,,$$

oder auch

$$-u\lg\frac{1}{x} + \lg\lg\frac{1}{x} = \lg\lg\frac{1}{u}\,.$$

V, 57 Wird noch $\lg\frac{1}{x} = \xi$, $\frac{1}{u} = v$ gesetzt, so genügt es also zu zeigen, daß die Gleichung

$$\varphi(v) = \lg\lg v + \frac{\xi}{v} - \lg\xi = 0,$$

wo ξ fest im Intervall $0 < \xi \leqq e$ ist, im Intervall $v > 1$ nur eine einzige Lösung hat. Dazu bilde ich

$$\varphi'(v) = \frac{1}{v\lg v} - \frac{\xi}{v^2} = \frac{1}{v}\left(\frac{1}{\lg v} - \frac{\xi}{v}\right).$$

Das Vorzeichen von $\varphi'(v)$ stimmt mit dem von

$$\psi(v) = \frac{v}{\xi} - \lg v$$

überein. Nun ist

$$\psi'(v) = \frac{1}{\xi} - \frac{1}{v}\left\{\begin{array}{lll} < 0 & \text{für} & v < \xi \\ = 0 & \text{"} & v = \xi \\ > 0 & \text{"} & v > \xi \end{array}\right\}.$$

also

$$\psi(v) \left\{ \begin{array}{lll} \text{fällt} & \text{für} & v < \xi \\ \text{Minimum} & \text{"} & v = \xi \\ \text{wächst} & \text{"} & v > \xi \end{array} \right\}.$$

Ist nur a.) $\mathbf{0 < \xi \leqq 1}$, so ist $\psi(v)$ wegen $v > 1$ stets wachsend, und da $\psi(1) = \frac{1}{\xi} > 0$ ist, gilt allgemein

$$\psi(v) > 0\,, \quad \text{d. h.} \quad \varphi'(v) > 0 \quad \text{für} \quad v > 1.$$

In diesem Falle hat also $\varphi(v) = 0$ nur eine einzige Lösung. Ist aber b.) $\mathbf{1 < \xi \leqq e}$, so fällt das Minimum $v = \xi$ von $\psi(v)$ in das Intervall $v > 1$. Es hat den Wert

$$\psi(\xi) = 1 - \lg \xi \geqq 1 - \lg e = 0,$$

sodaß auch hier stets

$$\psi(v) \geqq 0, \quad \text{d. h.} \quad \varphi'(v) \geqq 0 \quad \text{für} \quad v > 1$$

gilt, und somit wieder $\varphi(v) = 0$ nur eine einzige Lösung hat.

6.) $\mathbf{0 < x < \left(\frac{1}{e}\right)^{e}}$. Angenommen, es existierte ein Grenzwert, so wäre dieser nach 1.), 2.) $< \frac{1}{e}$. V, 58
Also gälte insbesondere

$$f_{2n+1}(x) < \frac{1}{e} \qquad (n \geqq n_0).$$

Ich zeige im Gegensatz dazu:

$$f_{2n+1}(x) \geqq \frac{1}{e} \qquad (n \geqq 0).$$

Zunächst ist nämlich

$$f_1(x) = 1 > \frac{1}{e}.$$

Wird ferner die Richtigkeit für ein $n \geqq 0$ angenommen, so folgt

$$\begin{aligned} f_{2n+3}(x) = x^{x^{f_{2n+1}(x)}} &\geqq \left(e^{-\frac{1}{f_{2n+1}(x)}}\right)^{\left(e^{-\frac{1}{f_{2n+1}(x)}}\right)^{f_{2n+1}(x)}} \\ &= e^{-\frac{1}{f_{2n+1}(x)}\cdot e^{-1}} \geqq e^{-1}, \end{aligned}$$

wenn nur gezeigt wird, daß

$$\varphi(x) = x^{x^\eta} \qquad (\eta > 0)$$

sein absolutes Minimum für $x = e^{-\frac{1}{\eta}}$ annimmt. Das bestätigt man aber ohne Schwierigkeit durch Betrachtung der 1. und 2. Ableitung.

5.7 Analytische Behandlung von $x^2 - Dy^2 = -1$. (18.7.1928)

Analytic treatment of the negative Pell equation, jointly with Bessel-Hagen.

V, 59

(Gemeinsam mit Dr. Bessel–Hagen).

1.) Sei D eine quadratfreie positive ganze Zahl. Wir bilden aus der Thetafunktion

$$\vartheta(z) = \sum_m z^{m^2} \qquad \text{(konv. für } |z| < 1)$$

die beiden Funktionen

$$\begin{aligned} \vartheta(rz) &= \sum_m r^{m^2} z^{m^2} \qquad \text{(konv. für } |z| < r^{-1}) \\ \vartheta\left(\frac{r^D}{z^D}\right) &= \sum_n r^{Dn^2} z^{-Dn^2} \qquad \text{(konv. für } r < |z|). \end{aligned}$$

Dabei sei

$$0 < r < 1,$$

sodaß beide Reihendarstellungen den Ring

$$r < |z| < r^{-1}$$

zum gemeinsamen Konvergenzgebiet haben. Es ist daher

$$\psi(r) = \sum_{m^2 - Dn^2 = -1} r^{m^2 + Dn^2} = \frac{1}{2\pi i} \int_{|z|=1} \vartheta(rz)\vartheta\left(\frac{r^D}{z^D}\right) dz.$$

2.) Zur Abschätzung des Integrals sei auf $|z| = 1$ eine Farey–Teilung der Ordnung N zugrundegelegt. Ist $\frac{p}{q}$ einer der Farey–Brüche, so sei

V, 60

$$\varepsilon = \varepsilon\left(\frac{p}{q}\right) = e^{2\pi i \frac{p}{q}}$$ der zugehörige Teilpunkt auf $|z| = 1$

$$z = \varepsilon e^{i\Theta}, \quad -\Theta' \leqq \Theta \leqq +\Theta''$$

die Parameterdarstellung des zugehörigen Bogens, der durch die Radianten begrenzt ist, d. h.

$$\frac{2\pi}{2qN} \leqq \Theta' = 2\pi\left(\frac{p}{q} - \frac{p+p'}{q+q'}\right) = 2\pi\frac{1}{q(q+q')} < \frac{2\pi}{qN}$$

$$\frac{2\pi}{2qN} \leqq \Theta'' = 2\pi\left(-\frac{p}{q} + \frac{p+p''}{q+q''}\right) = 2\pi\frac{1}{q(q+q'')} < \frac{2\pi}{qN}$$

wenn $\frac{p'}{q'}$, $\frac{p''}{q''}$ linker und rechter Nachbar von $\frac{p}{q}$ in der Farey–Reihe sind.

Es werde ferner eine Scheidung in kleine und große Bögen vorgenommen:

große Bögen: $1 \leqq q < N^\beta$
kleine Bögen: $N^\beta \leqq q \leqq N$,

wo β eine noch näher zu bestimmende, den Ungleichungen

$$0 < \beta < 1$$

genügende Zahl ist.

Schließlich sei

$$\varrho = N^{-\alpha}$$

mit einem noch näher zu bestimmenden $\alpha > 0$ gesetzt.

V, 61 3.) Es werde noch gesetzt:

$$r = e^{-\varrho}, \quad z_1 = e^{-\frac{\pi^2}{q^2}\frac{1}{\varrho - i\Theta}}, \quad z_2 = e^{-\frac{\pi^2}{q^2}\frac{1}{\varrho + i\Theta}}$$

$$G_1 = G\left(\frac{p}{q}\right) = \sum_{h=0}^{q-1} \varepsilon^{h^2}, \quad G_2 = G\left(\frac{-Dp}{q}\right) = \sum_{k=0}^{q-1} \varepsilon^{-Dk^2}.$$

Dann ergibt die Thetatransformation:

$$\begin{aligned}
\varrho(rz) &= \sum_m \varepsilon^{m^2} e^{-(\varrho - i\Theta)m^2} = \sum_{h=0}^{q-1} \varepsilon^{h^2} \sum_m e^{-q^2(\varrho - i\Theta)(m+\frac{h}{q})^2} \\
&= \frac{\sqrt{\pi}}{q} \frac{1}{\sqrt{\varrho - i\Theta}} \sum_{h=0}^{q-1} \varepsilon^{h^2} \sum_m e^{2\pi i m \frac{h}{q}} z_1^{m^2} \\
&= \frac{\sqrt{\pi}}{q} H_1 \frac{1}{\sqrt{\varrho - i\Theta}} + \frac{\sqrt{\pi}}{q} \frac{1}{\sqrt{\varrho - i\Theta}} \sum_{h=0}^{q-1} \varepsilon^{h^2} \sum_{m \neq 0} e^{2\pi i m \frac{h}{q}} z_1^{m^2} \\
&= \frac{\sqrt{\pi}}{q} H_1 \frac{1}{\sqrt{\varrho - i\Theta}} + \mathfrak{R}_1\,,
\end{aligned}$$

ebenso

$$\begin{aligned}
\vartheta\left(\frac{r^D}{z^D}\right) &= \frac{1}{\sqrt{D}} \frac{\sqrt{\pi}}{q} H_2 \frac{1}{\sqrt{\varrho + i\Theta}} + \frac{1}{\sqrt{D}} \frac{\sqrt{\pi}}{q} \frac{1}{\sqrt{\varrho + i\Theta}} \cdot \\
&\quad \cdot \sum_{k=0}^{q-1} \varepsilon^{-Dk^2} \sum_{m \neq 0} e^{2\pi i m \frac{k}{q}} z_2^{m^2} \\
&= \frac{1}{\sqrt{D}} \frac{\sqrt{\pi}}{q} H_2 \frac{1}{\sqrt{\varrho + i\Theta}} + \mathfrak{R}_2\,.
\end{aligned}$$

4.) Es entspreche jetzt q einem *großen Bogen*, und es sei z auf diesem variabel. Dann ist V, 62

$$\begin{aligned}
\left.\begin{array}{l} |z_1| \\ |z_2| \end{array}\right\} &= \exp\left(-\frac{\pi^2}{q^2} \frac{\varrho}{\varrho^2 + \Theta^2}\right) < \exp\left(-\frac{\pi^2}{q^2} \frac{\varrho}{\varrho^2 + 4\pi^2 \frac{1}{q^2 N^2}}\right) \\
&= \exp\left(-\frac{\pi^2}{q^2 \varrho + 4\pi^2 \frac{1}{N^2 \varrho}}\right) \\
&< \exp\left(-\frac{\pi^2}{N^{2\beta-\alpha} + 4\pi^2 N^{\alpha-2}}\right).
\end{aligned}$$

Für $N \to \infty$ geht dies $\to 0$, wenn nur

$$2\beta < \alpha < 2.$$

Dann gilt also

$$\left|\sum_{m\neq 0} z_1^{m^2} e^{2\pi i m\frac{h}{q}}\right| < a_1|z_1| < a_1 \exp\left(-\frac{\pi^2}{N^{2\beta-\alpha}+4\pi^2N^{\alpha-2}}\right)$$

wenn nur $N > N_0$, wo a_1 und N_0 absolute Konstanten sind,

und somit für jedes $\varepsilon > 0$

$$\left|\sum_{m\neq 0} z_1^{m^2} e^{2\pi i m\frac{h}{q}}\right| < A_1 e^{-N^{\mu-\varepsilon}},$$

wo A_1 eine nur von ε abhängige Konstante und

$$\mu = \operatorname{Min}(\alpha-2\beta, 2-\alpha) > 0.$$

V, 63 Daraus folgt

$$\begin{aligned} |\mathfrak{R}_1| &< \frac{\sqrt{\pi}}{q}\frac{1}{\sqrt{\varrho}} q A_1 e^{-N^{\mu-\varepsilon}} \\ &= A_2 N^{\frac{\alpha}{2}} e^{-N^{\mu-\varepsilon}}, \end{aligned}$$

also auch

$$|\mathfrak{R}_1| < A_3 e^{-N^{\mu-\varepsilon}}.$$

Ebenso folgt

$$|\mathfrak{R}_2| < A_4 e^{-N^{\mu-\varepsilon}}.$$

Für den Integranden ergibt sich daraus

$$\vartheta(rz)\vartheta\left(\frac{r^D}{z^D}\right) = \frac{\pi}{\sqrt{D}}\frac{G_1G_2}{q^2}\frac{1}{\sqrt{\varrho^2+\Theta^2}} + \mathfrak{R}_3$$

mit

$$\begin{aligned} |\mathfrak{R}_3| &\leqq |\mathfrak{R}_1|\cdot\frac{\sqrt{\pi}}{\sqrt{D}}\frac{|G_2|}{q}\frac{1}{\sqrt{\varrho}} + |\mathfrak{R}_2|\cdot\sqrt{\pi}\frac{|G_1|}{q}\frac{1}{\sqrt{\varrho}} + |\mathfrak{R}_1|\cdot|\mathfrak{R}_2| \\ &< A_5\frac{1}{\sqrt{q}\sqrt{\varrho}}e^{-N^{\mu-\varepsilon}} + A_6\frac{1}{\sqrt{q}\sqrt{\varrho}}e^{-N^{\mu-\varepsilon}} + A_7 e^{-2N^{\mu-\varepsilon}}, \end{aligned}$$

also wegen $\frac{1}{\sqrt{q}\sqrt{\varrho}} < \frac{1}{\sqrt{\varrho}} = N^{\frac{\alpha}{2}}$ wieder

$$|\mathfrak{R}_3| < A_8 e^{-N^{\mu-\varepsilon}}.$$

5.) Es werde weiterhin ein *großer Bogen* betrachtet. Das Integral über ihn ist

$$\mathfrak{I} = \mathfrak{I}\left(\frac{p}{q}\right) = \frac{1}{2\pi i}\int\limits_{-\Theta'}^{+\Theta''} \frac{\pi}{\sqrt{D}}\,\frac{G_1 G_2}{q^2}\,\frac{1}{\sqrt{\varrho^2+\Theta^2}}\varepsilon i e^{i\Theta} d\Theta + \frac{1}{2\pi i}\int\limits_{-\Theta'}^{+\Theta''} \mathfrak{R}_3 \varepsilon i e^{i\Theta} d\Theta$$

V, 64

Mit

$$b = b\left(\frac{p}{q}\right) < 2\frac{2\pi}{qN}$$

sei die Länge des Bogens bezeichnet. Dann ist

$$\mathfrak{I} = \frac{\varepsilon}{\sqrt{D}}\,\frac{G_1 G_2}{q^2}\cdot\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''} \frac{e^{i\Theta} d\Theta}{\sqrt{\varrho^2+\Theta^2}} + \mathfrak{R}_4\,,$$

wo

$$|\mathfrak{R}_4| = \left|\frac{1}{2\pi i}\int\limits_{-\Theta'}^{\Theta''} \mathfrak{R}_3 \varepsilon i e^{i\Theta} d\Theta\right| \leqq \frac{b}{2\pi}\cdot|\mathfrak{R}_3| < \frac{b}{2\pi} A_8 e^{-N^{\mu-\varepsilon}}.$$

Es werde nun erstens das

$$\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''} \frac{e^{i\Theta} d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

durch das

$$\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

ersetzt. Der dabei an $\mathfrak{J}$ auftretende Faktor ist seinem Betrage nach

$$|\mathfrak{R}_5| = \left|\frac{\varepsilon}{\sqrt{D}}\,\frac{G_1G_2}{q^2}\right| \cdot \left|\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''} \frac{e^{i\Theta}-1}{\sqrt{\varrho^2+\Theta^2}}d\Theta\right|$$

V, 65

Da nun, wie schon oben benutzt,

$$|G_1| \leqq \sqrt{2}\sqrt{q}\,, \quad |G_2| \leqq \sqrt{2}\sqrt{q}\,,$$

so folgt

$$\begin{aligned}
|\mathfrak{R}_5| \;&\leqq\; \frac{2}{\sqrt{D}}\,\frac{1}{q}\cdot\int\limits_{-\Theta'}^{+\Theta''}\frac{\left|\sin\frac{\Theta}{2}\right|}{\sqrt{\varrho^2+\Theta^2}}d\Theta \\
&<\; \frac{2}{\sqrt{D}}\,\frac{1}{q}\cdot\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''}\frac{|\Theta|}{\sqrt{\varrho^2+\Theta^2}}d\Theta \\
&<\; \frac{2}{\sqrt{D}}\,\frac{1}{q}\cdot\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''}d\Theta = \frac{2}{\sqrt{D}}\,\frac{1}{q}\cdot\frac{b}{2} \\
&<\; \frac{2}{\sqrt{D}}\,\frac{1}{q}\cdot\frac{2\pi}{qN} = a_2\frac{1}{N}\cdot\frac{1}{q^2}
\end{aligned}$$

Zweitens werde das

$$\frac{1}{2}\int\limits_{-\Theta'}^{+\Theta''}\frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

durch das

$$\frac{1}{2}\int\limits_{-\pi}^{+\pi}\frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

ersetzt. Der dabei auftretende Fehler ist seinem Betrage nach

$$|\mathfrak{R}_6| = \left|\frac{1}{2}\left\{\int\limits_{\Theta''}^{\pi} + \int\limits_{-\Theta'}^{-\pi}\right\}\frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}\right|$$

V, 66

$$= \int_{\Theta''}^{\pi} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}} < \int_{\frac{\pi}{qN}}^{\pi} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

$$= \log \frac{\pi + \sqrt{\varrho^2+\pi^2}}{\frac{\pi}{qN} + \sqrt{\varrho^2 + \frac{\pi^2}{q^2N^2}}}$$

$$= \left\{ \log qN + \log \frac{\pi + \sqrt{\varrho^2+\pi^2}}{\pi + \sqrt{(\varrho qN)^2+\pi^2}} \right\}$$

Wird nun

$$\beta + 1 < \alpha$$

gewählt, sodaß $\varrho qN < N^{-\alpha+\beta+1} \to 0$ mit $N \to \infty$, so wird hiernach

$$\mathfrak{R}_6 < \log qN + O(1) < (1+\beta)\log N + O(1)$$

Dagegen hat das volle Integral

$$\frac{1}{2}\int_{-\pi}^{+\pi} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}}$$

den Wert

$$\begin{aligned} \int_0^{\pi} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}} &= \log \frac{\pi + \sqrt{\varrho^2+\pi^2}}{\varrho} \\ &= \log \varrho^{-1} + O(1) \\ &= \alpha \log N + O(1), \end{aligned}$$

sodaß obiger Fehler jedenfalls in der Konstanten vor $\log N$ kleiner ist. Die Bedingungen

V, 67

$$0 < \beta < 1, \quad \alpha > 0, \quad 2\beta < \alpha < 2, \quad \beta + 1 < \alpha$$

sind miteinander verträglich.

Wir erhalten somit:

$$\mathfrak{I} = \frac{\varepsilon}{\sqrt{D}} \frac{G_1G_2}{q^2} \cdot \left(\int_0^{\pi} \frac{d\Theta}{\sqrt{\varrho^2+\Theta^2}} + \mathfrak{R}_6 \right) + \mathfrak{R}_5 + \mathfrak{R}_4 \,.$$

Jetzt werde über alle großen Bögen summiert. Für den zugehörigen Beitrag $\psi_1(r)$ zu $\psi(r)$ gilt dann:

$$\psi_1(r) = \sum_{q=1}^{N^\beta} \sum_p \frac{\varepsilon}{\sqrt{D}} \frac{G_1 G_2}{q^2} \left(\int\limits_0^\pi \frac{d\Theta}{\sqrt{\varrho^2 + \Theta^2}} + \mathfrak{R}_6 \right) + \mathfrak{R}_7 \,,$$

wo

$$\begin{aligned} |\mathfrak{R}_7| &\leqq \sum_{q,p} |\mathfrak{R}_5| + \sum_{q,p} |\mathfrak{R}_4| \\ &< a_2 \frac{1}{N} \sum_q \frac{\varphi(q)}{q^2} + \frac{A_8}{2\pi} e^{-N^{\mu-\varepsilon}} \sum_{q,p} b \\ &< a_2 \frac{1}{N} \sum_q \frac{1}{q} + A_8 e^{-N^{\mu-\varepsilon}} \\ &< a_3 \frac{\log N}{N} \,. \end{aligned}$$

Kapitel 6

Tagebuch VI: Oktober 1928 – 1929

Eintragungen

6.1 Invariantenkörper. (3.10.1928)

Let K be a field and suppose that Hilbert's irreducibility theorem holds over K (for instance, $K = \mathbb{Q}$). Emmy Noether has observed that it would be possible to construct field extensions $L|K$ with a given permutation group G as Galois group provided the field of invariants of G is rational over K [Noe17]*. Hasse mentions this rationality property (for an arbitrary group G) as a conjecture, referring to a coversation with Artin. (Hasse had met Artin at the annual meeting of the "Deutsche Mathematiker Vereinigung" in Hamburg in September 1928.) We observe that later in 1930 Wolfgang Franz, one of Hasse's students, submitted his Ph.D. thesis where he developed a general theory of fields over which Hilbert's irreducibility theorem holds* [Fra31]*. (Today such fields are called "Hilbert fields"). It can be assumed that Franz had obtained the topic of his thesis from Hasse who remembered the conversation with Artin. The general rationality conjecture for the field of invariants has been refuted in the meantime. See* [Swa69]*. The papers by S. Breuer which Hasse mentions are concerned with the field of invariants for certain metacyclic groups (see, e.g.,* [Bre24]*).*

VI, 3

(3. X. 28)

(Nach mündlicher Mitteilung von E. Artin).

Sei K beliebiger Grundkörper, $L = K(x_1, \ldots, x_n)$ mit $x_1, \ldots, x_n$ als Unbestimmten.

Sei $\mathfrak{G}$ eine beliebige Permutationsgruppe (oder endliche Substitutionsgruppe in K) für $x_1, \ldots, x_n$. Dann gehört dazu ein invarianter Unterkörper $\mathfrak{I}$ von L.

Es besteht die Vermutung, daß $\mathfrak{I}/K \cong L/K$ ist, d. h. *daß es genau n algebraisch unabhängige Invarianten zu $\mathfrak{G}$ in L gibt.*

Ist speziell $\mathfrak{G}$ die symmetrische Permutationsgruppe, so stimmt das bekanntlich.

Ist jene Vermutung richtig, so gibt es über K Körper mit der Gruppe $\mathfrak{G}$, sofern die Anwendung des Irreduzibilitätssatzes klappt, also z. B. wenn K ein endl. algebr. Zahlkörper ist.

Überdies bekommt man Parameterdarstellungen der betr. Gleichungen durch die n algebraisch unabhängigen Invarianten.

Literatur hierzu: E. Noether, S. Breuer

6.2 Projektive Geometrie und Schiefkörper. (3.10.1928)

Projective geometry and division algebras according to Artin. Hasse cites Hilbert [Hil99] *and Hessenberg* [Hes04]. *Compare with Artin's later book on Geometric Algebra* [Art57]. *Like the foregoing entry this is entry has been written after Hasse had met Artin on the annual meeting of the* "Deutsche Mathematiker Vereinigung" *in Hamburg at the end of September.*

VI, 4

(3. X. 28)

(Nach mündlicher Mitteilung von E. Artin).

Wenn ein Schiefkörper K gegeben ist, so läßt sich zu ihm eine ebene projektive Geometrie bilden, indem man in üblicher Weise die Elementtripel (x, y, z) aus K Punkte und die Linearformen $ux + vy + wz$ aus K Geraden nennt. Es genügt dabei völlig, sich auf die Ebene zu beschränken, da sich eine ebene projektive Geometrie nur auf eine einzige Art in den Raum fortsetzen läßt etz. Man überzeugt sich, daß bei der genannten Deutung alle Inzidenz–Axiome der ebenen projektiven Geometrie, insbesondere das Desarguesche, erfüllt sind. Umgekehrt läßt sich auch jede Realisierung dieser Axiome in der angegebenen Weise aus einem eindeutig bestimmten Schiefkörper K herleiten.

Dem kommutativen Gesetz in K entspricht dabei der Pascalsche Satz.

Literatur: Hilbert, Grundlagen der Geometrie
Hessenberg, Acta Mathematica

6.3 Hölder's Satz über Gruppenerweiterung. (3.10.1928)

Extensions of an abelian group with a cyclic factor group. This note resulted from a coversation with Otto Schreier. Apparently this note is preparing the note 6.6 on Artin's reciprocity law.]

VI, 5

(3. X. 28)

(Nach mündlicher Mitteilung von O. Schreier).

Gegeben sei eine Abelsche Gruppe $\mathfrak{H}$. Damit durch Hinzunahme eines Elementes S eine Gruppe $\mathfrak{G}$ entsteht, die $\mathfrak{H}$ als Normalteiler mit von der Ordnung n zyklischer Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ enthält, muß gesetzt werden:

$$\mathsf{S}^n = A \quad \text{aus} \quad \mathfrak{H} \tag{1}$$

$$\mathsf{S}^{-1} A_i \mathsf{S} = A_{s_i} \quad \text{aus } \mathfrak{H} \text{ für jedes } A_i \text{ aus } \mathfrak{H}. \tag{2}$$

Dann und nur dann wird das angegebene Ziel auf diese Weise erreicht, wenn $\binom{A_i}{A_{s_i}}$ ein Automorphismus von $\mathfrak{H}$ ist, dessen Ordnung Teiler von n ist, und bei dem A fest bleibt.

Für unendliches n fallen die beiden letzten Zusatzbedingungen einfach fort.

Literatur: Die Arbeiten von O. Schreier

6.4 Zum expliziten Reziprozitätsgesetz der ℓ–ten Potenzreste im ℓ–ten Kreiskörper. (16.10.1928)

This connects to the earlier entry of October 4, 1927.] There, Hasse had used the method of Eisenstein to obtain an explicit formula for the general reciprocity law for the prime power ℓ^n in the field of ℓ^n-th roots of unity. Here, Hasse applies this method to the special case $n = 1$ where the formulas and the computations are much simplified. This yields a partial improvement of Hasse's paper [Has25a]. *Hasse mentions that it was Artin who had suggested to write down this new version. We note that Hasse had met Artin in September 1928 at the annual meeting of the "Deutsche Mathematiker Vereinigung" in Hamburg. It seems that on that occasion Artin had also suggested to prepare the paper with the general formulas for ℓ^n which Hasse had obtained in his earlier entry of October 4, 1927. At that time Hasse had sent the manuscript too to Artin but refrained from submitting it for publication since he was not yet quite satisfied with the form of his formulas (see* [FR08], *section 17.3). Now he followed Artin's suggestion. He submitted the manuscript on November 4, 1928, to the "Hamburger Abhandlungen"* [Has29]. *See also the entry 7.3 of December 1931.]*

VI, 6

(16. X. 28)

(Einer Anregung Artin's zufolge ausgearbeitet).

Sei ℓ ungerade Primzahl, ζ primitive ℓ–te Einheitswurzel, $\lambda = 1 - \zeta$ und k der Körper der ℓ–ten Einheitswurzeln.

α sei eine für λ ganze Zahl aus k,

$$\alpha = \varphi(\zeta)$$

eine Darstellung als Polynom in ζ mit für ℓ ganzen rationalen Koeffizienten. Dann werde

$$\frac{\alpha}{\alpha'} = \frac{\varphi'(\zeta)}{\varphi(\zeta)} = \left.\frac{\frac{d}{dx}\varphi(x)}{\varphi(x)}\right|_{x=\zeta}$$

gesetzt. Ist auch

$$\alpha = \psi(\zeta),$$

so gilt

$$\varphi(x) = \psi(x) + \frac{x^\ell - 1}{x - 1} g(x),$$

wo $g(x)$ ein Polynom mit für ℓ ganzen Koeffizienten ist. Also

$$\varphi'(\zeta) = \psi'(\zeta) + \frac{\ell\zeta^{-1}}{\zeta - 1} g(\zeta) \equiv \psi'(\zeta) \text{ mod. } \frac{\ell}{\lambda}$$

Somit auch

$$\frac{\varphi'(\zeta)}{\varphi(\zeta)} \equiv \frac{\psi'(\zeta)}{\psi(\zeta)} \text{ mod. } \frac{\ell}{\lambda}\,,$$

VI, 7 wenn α sogar prim zu λ ist.

Für zu λ prime α hat also $\frac{\alpha'}{\alpha}$ mod. $\frac{\ell}{\lambda}$ einen eindeutigen Sinn. Es gilt daher auch

$$\frac{(\alpha_1\alpha_2)'}{\alpha_1\alpha_2} \equiv \frac{\alpha_1'}{\alpha_1} + \frac{\alpha_2'}{\alpha_2} \text{ mod. } \frac{\ell}{\lambda}\,.$$

Nun sei

$$\eta_a = 1 - \lambda^a\,, \quad \left(\frac{\eta_a, \eta_b}{\lambda}\right)^{-1} = \zeta^{[\eta_a, \eta_b]}$$

gesetzt. Dann gilt nach Tagebuch V, S. 13]:

$$[\eta_a, \eta_b] \equiv \sum_{(p,q)=1} (p'a + q'b) \frac{1}{\ell} S\left(-\frac{\zeta}{\lambda} \log \eta_{pa+qb}\right) \text{ mod. } \ell.$$

Es seien a und b prim zu ℓ vorausgesetzt. Dann verschwinden mod. ℓ die Glieder mit $p \equiv 0$ (ℓ) oder $q \equiv 0$ (ℓ), ferner die mit $pa + qb \not\equiv 0$ (ℓ), während in denen mit $pa + qb \equiv 0$ (ℓ) gilt

$$p'a + q'b \equiv \frac{b}{p} \equiv -\frac{a}{q} \text{ mod. } \ell.$$

Also

$$[\eta_a, \eta_b] \equiv \sum_{\substack{(p,q)=1 \\ (p,\ell)=1 \\ (q,\ell)=1}} \frac{-a}{q} \frac{1}{\ell} S\left(-\frac{\zeta}{\lambda} \log \eta_{pa+qb}\right) \mod. \ell$$

$$\equiv \frac{1}{\ell} S\left(\zeta \sum_{\substack{(p,q)=1 \\ (p,\ell)=1 \\ (q,\ell)=1}} \sum_{m=1}^{\infty} \frac{-a}{mq} \lambda^{m(pa+qb)-1}\right) \mod. \ell$$

Die Summation kann auf $(m, \ell) = 1$ beschränkt werden,weil $pa + qb \geqq 2$ und $\frac{\zeta\lambda^{2\ell-1}}{\ell}, \frac{\zeta\lambda^{2\ell^2-1}}{\ell^2}, \dots$ durch ℓ^2 teilbare Spuren haben. Also: VI, 8

$$[\eta_a, \eta_b] \equiv \frac{1}{\ell} S\left(\zeta \sum_{(P,\ell)=1} \sum_{(Q,\ell)=1} \frac{-a}{Q} \lambda^{Pa+Qb-1}\right) \mod. \ell$$

$$\equiv \frac{1}{\ell} S\left(\zeta \sum_{(P,\ell)=1} (-a)\lambda^{Pa-1} \sum_{(Q,\ell)=1} \frac{\lambda^{Qb}}{Q}\right) \mod. \ell$$

Ist $b > 1$, so kann die Summation nach Q ähnlich wie eben, jetzt wieder über alle Q erstreckt werden. Desgleichen kann die Summation nach P stets über alle P erstreckt werden, weil die $\sum_Q \equiv 0 \mod. \lambda^2$ ist. Somit:

$$[\eta_a, \eta_b] \equiv \frac{1}{\ell} S\left(\zeta \cdot -a \sum_{P=1}^{\infty} \lambda^{Pa-1} \cdot -\log \eta_b\right) \mod. \ell$$

Nun ist

$$-a \sum_{P=1}^{\infty} (1-x)^{Pa-1} = \frac{d}{dx} \sum_{P=1}^{\infty} \frac{(1-x)^{Pa}}{P} = -\frac{d}{dx} \log\big(1-(1-x)\big)$$
$$= \frac{-\frac{d}{dx}\big(1-(1-x)^a\big)}{1-(1-x)^a}$$

Für $x = \zeta$ resultiert also

$$-a \sum_{P=1}^{\infty} \lambda^{Pa-1} \equiv -\frac{\eta_a'}{\eta_a} \mod. \frac{\ell}{\lambda},$$

und da $\log\eta_b \equiv 0 \mod \lambda^2$, so genügt diese Bestimmtheit mod. $\frac{\ell}{\lambda}$ unter dem
VI, 9 Spurzeichen. Es resultiert also:

$$[\eta_a, \eta_b] \equiv \frac{1}{\ell} S\left(\zeta \cdot \frac{\eta_a'}{\eta_a} \cdot \log\eta_b\right) \text{ mod. } \ell$$

für a, b prim zu ℓ, $b > 1$.

Daraus ergibt sich sofort:

$$[\alpha, \beta] \equiv \frac{1}{\ell} S\left(\zeta \cdot \frac{\alpha'}{\alpha} \cdot \log\beta\right) \text{ mod. } \ell$$

für $\alpha \equiv 1 \text{ mod. } \lambda$, $\beta \equiv 1 \text{ mod. } \lambda^2$.

Man muß dazu nur noch zeigen, daß der Ausdruck rechts für α oder $\beta = \eta_\ell$ verschwindet mod. ℓ. Für $\beta = \eta_\ell$ ist $\log\beta \equiv 0 \text{ mod. } \ell\lambda$, also diese Behauptung richtig. Für $\alpha = \eta_\ell = 1 - \lambda^\ell$ ist $x' \equiv -\ell \cdot \lambda^{\ell-1} \equiv 0 \text{ mod. } \frac{\ell}{\lambda}$, also $\frac{\alpha'}{\alpha} \equiv 0 \text{ mod. } \frac{\ell}{\lambda}$, woraus wiederum die Behauptung folgt. Schließlich ergibt sich noch, daß die Annahme $\alpha \equiv 1 \text{ mod. } \lambda$ entbehrlich ist, und durch α prim zu λ ersetzt werden kann, auf ganz ähnlichem Wege.

Also

$$[\alpha, \beta] \equiv \frac{1}{\ell} S\left(\zeta \cdot \frac{\alpha'}{\alpha} \cdot \log\beta\right) \text{ mod. } \ell$$

für α prim zu λ, $\beta \equiv 1 \text{ mod. } \lambda^2$.

Auch für $\alpha = \lambda$ gilt

$$[\lambda, \beta] \equiv \frac{1}{\ell} S\left(\zeta \cdot \frac{\lambda'}{\lambda} \cdot \log\beta\right) \text{ mod. } \ell$$

für $\beta \equiv 1 \text{ mod. } \lambda$,

wenn $\frac{\lambda'}{\lambda} = \left.\frac{\frac{d}{dx} 1-x}{1-x}\right|_{x=\zeta}$ gesetzt wird.

6.5 Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. (Oktober 1928)

Hasse develops the theory of cubic number fields on a class field theoretic basis. Already in September 1927 Hasse had sent a manuscript on this to Arnold Scholz. In April 1929 he sent the manuscript to the "Mathematische Zeitschrift" for publication where it appeared 1930 [Has30a]. *Parallel to this Hasse had one of his Ph.D. students, H. Reichardt, develop the theory of cubic fields generated as Kummer fields over a biquadratic subfield (Cardano's formula!). This was completed in 1930 in* [Rei33].

VI, 10

(Oktober 1928)

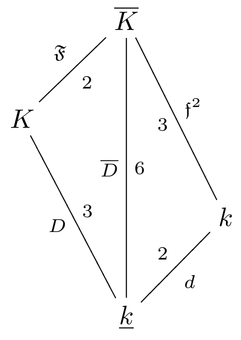
Bezeichnungen.

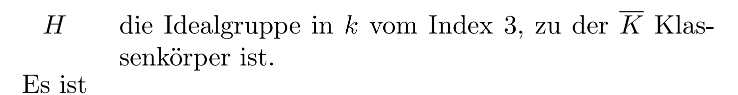
$\underline{k}$	rationaler Zahlkörper.
K, K_1, K_2	drei konjugierte kubische Zahlkörper, die als **verschieden** vorausgesetzt werden. (Im Folgenden ist „kubischer Zahlkörper“ stets in diesem Sinne gemeint, d. h. es sind die Galoisschen, also zyklischen ausgeschlossen).
D	ihre Diskriminante.
$\overline{K} = (K, K_1, K_2) = K(\sqrt{D})$	der zugehörige bikubische Galoissche Körper.
$\overline{D}$	seine Diskriminante.
$k = \underline{k}(\sqrt{D})$	der in $\overline{K}$ enthaltene quadratische Körper.
d	seine Diskriminante, also auch $k = \underline{k}(\sqrt{d})$ und $$D = df^2$$ mit ganzem, rationalem f.
$(\sqrt{d} \to -\sqrt{d}\,)$	wird durch Striche angedeutet: $\tau\alpha = \alpha'$, $\tau\mathfrak{a} = \mathfrak{a}'$.
$\mathfrak{f}^2$	die Relativdiskriminante von $\overline{K}/k$
$\mathfrak{F}$	die Relativdiskriminante von $\overline{K}/K$.

Es ist

$$|\overline{D}| = |d|^3 N(\mathfrak{f})^2,$$
$$|\overline{D}| = |D|^2 N(\mathfrak{F}).$$

VI, 11





H die Idealgruppe in k vom Index 3, zu der $\overline{K}$ Klassenkörper ist.

Es ist

$\mathfrak{f}$ ihr Führer.

Die Anwendung der Hilbertschen Theorie der relativ–Galoisschen Zahlkörper verbunden mit der Takagischen Theorie der relativ–Abelschen Zahlkörper führt, wie gleich näher erläutert wird, zu den in der umstehenden Tabelle zusammengestellten Möglichkeiten und Bedingungen für die Zerlegung der Primzahlen aus $\underline{k}$ in $\overline{K}, k, K$ und ihre Beiträge zu $\overline{D}, \mathfrak{f}, d, \mathfrak{F}, D$.

Erläuterungen zur Tabelle.

Es bezeichnet:

$\mathfrak{S}$ die symmetrische Gruppe von drei Elementen.

$\mathfrak{A}$ die alternierende Gruppe, die in $\mathfrak{S}$ als Normalteiler steckt.

$\mathfrak{T}, \mathfrak{T}_1, \mathfrak{T}_2$ die drei verschiedenen konjugierten Untergruppen von $\mathfrak{S}$.

$\mathfrak{E}$ die identische Untergruppe von $\mathfrak{S}$.

$\mathfrak{S}$ ist die Galoissche Gruppe von $\overline{K}/\underline{k}$. Den Untergruppen

$$\mathfrak{E}\,; \quad \mathfrak{A}\,; \quad \mathfrak{T}, \mathfrak{T}_1, \mathfrak{T}_2\,; \quad \mathfrak{S}$$

von $\mathfrak{S}$ sind im Sinne des Fundamentalsatzes der Galoisschen Theorie die Teilkörper

$$\overline{K}\,; \quad k\,; \quad K, K_1, K_2\,; \quad \underline{k}$$

von $\overline{K}$ zugeordnet.

In Spalte 1 sind alle Möglichkeiten für die „Hilbertsche Untergruppenreihe“ in $\overline{K}/\underline{k}$ der Primideale aus $\overline{K}$ aufgeführt. Es sind das alle Untergruppenreihen:

VI, 12

(Fortsetzung S. 14])

	Hilbertsche Untergruppenreihe							Primidealzerlegung von p in					
								$\overline{K}$		k		K	
	$\mathfrak{G}$	$\mathfrak{G}_Z$	$\mathfrak{G}_T$	$\mathfrak{G}_{V_1}$	$\cdots$	$\mathfrak{G}_{V_\nu}$	$\mathfrak{G}_{V_{\nu+1}}$	Faktoren	Grad	Fakt.	Gr.	Fakt.	Gr.
1	$\mathfrak{S}$	$\mathfrak{E}$	$\mathfrak{E}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}_1\overline{\mathfrak{P}}_2\cdot$ $\cdot\overline{\mathfrak{P}}'\overline{\mathfrak{P}}_1'\overline{\mathfrak{P}}_2'$	1	$\mathfrak{p}\mathfrak{p}'$	1	$\mathfrak{P}\mathfrak{P}_1\mathfrak{P}_2$	1
2	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{E}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}'$	3	$\mathfrak{p}\mathfrak{p}'$	1	$\mathfrak{P}$	3
3	$\mathfrak{S}$	$\mathfrak{T}$	$\mathfrak{E}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}_1\overline{\mathfrak{P}}_2$	2	$\mathfrak{p}$	2	$\mathfrak{P}\mathfrak{P}_1$	$1, 2$
4	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{A}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$(\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}')^3$	1	$\mathfrak{p}\mathfrak{p}'$	1	$\mathfrak{P}_3^3$	1
5	$\mathfrak{S}$	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}^3$	2	$\mathfrak{p}$	2	$\mathfrak{P}$	1
6	$\mathfrak{S}$	$\mathfrak{T}$	$\mathfrak{T}$	$\mathfrak{E}$	$\cdots$	$\mathfrak{E}$	$\mathfrak{E}$	$(\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}_1\overline{\mathfrak{P}}_2)^2$	1	$\mathfrak{p}^2$	1	$\mathfrak{P}\mathfrak{P}_1^2$	$1, 1$
7	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{A}$	$\mathfrak{A}$	$\cdots$	$\mathfrak{A}$	$\mathfrak{E}$	$(\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}')^3$	1	$\mathfrak{p}\mathfrak{p}'$	1	$\mathfrak{P}^3$	1
8	$\mathfrak{S}$	$\mathfrak{S}$	$\mathfrak{A}$	$\mathfrak{A}$	$\cdots$	$\mathfrak{A}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}^3$	2	$\mathfrak{p}$	2	$\mathfrak{P}^3$	1
9	$\mathfrak{S}$	$\mathfrak{S}$	$\mathfrak{S}$	$\mathfrak{A}$	$\cdots$	$\mathfrak{A}$	$\mathfrak{E}$	$\overline{\mathfrak{P}}^6$	1	$\mathfrak{p}^2$	1	$\mathfrak{P}^3$	1
10	$\mathfrak{S}$	$\mathfrak{T}$	$\mathfrak{T}$	$\mathfrak{T}$	$\cdots$	$\mathfrak{T}$	$\mathfrak{E}$	$(\overline{\mathfrak{P}}\,\overline{\mathfrak{P}}_1\overline{\mathfrak{P}}_2)^2$	1	$\mathfrak{p}^2$	1	$\mathfrak{P}\mathfrak{P}_1^2$	$1, 1$
	1							2		3		4	

VI, 13

	Bedingungen für p und seine Primfaktoren $\mathfrak{p}$ in k			Mögliche Werte von v
1	–	$\left(\frac{d}{p}\right) = +1$	$\mathfrak{p}, \mathfrak{p}'$ in H	–
2	–	$\left(\frac{d}{p}\right) = +1$	$\mathfrak{p}, \mathfrak{p}'$ nicht in H	–
3	–	$\left(\frac{d}{p}\right) = -1$	$\mathfrak{p}$ in H	–
4	$p \equiv +1\ (3)$	$\left(\frac{d}{p}\right) = +1$		–
5	$p \equiv -1\ (3)$	$\left(\frac{d}{p}\right) = -1$		–
6	$p \neq 2$	$\left(\frac{d}{p}\right) = 0$	$\mathfrak{p}$ in H	–
7	$p = 3$	$\left(\frac{d}{3}\right) = +1$		1
8	$p = 3$	$\left(\frac{d}{3}\right) = -1$		1
9	$p = 3$	$\left(\frac{d}{3}\right) = 0$		$1, 3$*)
10	$p = 2$	$\left(\frac{d}{2}\right) = 0$	$\mathfrak{p}$ in H	$1, 2$
	5	6	7	8

*) Es ist genauer: $v = 1$, wenn $3 | d$ und $\frac{d}{3} \equiv 1\ (3)$.

	Beitrag von p zu							
	$\overline{D}$	$\mathfrak{f}$	$N(\mathfrak{f})$	d	$\mathfrak{F}$	$N(\mathfrak{F})$	D	
1	–	–	–	–	–	–	–	
2	–	–	–	–	–	–	–	**I**
3	–	–	–	–	–	–	–	
4	p^4	$\mathfrak{p}\mathfrak{p}'$	p^2	1	1	1	p^2	
5	p^4	$\mathfrak{p}$	p^2	1	1	1	p^2	**II**
6	p^3	1	1	p	$\mathfrak{P}$	p	p	
7	3^8	$(\mathfrak{p}\mathfrak{p}')^2$	3^4	1	1	1	3^4	
8	3^8	$\mathfrak{p}^2$	3^4	1	1	1	3^4	
9	3^{2v+5}	$\mathfrak{p}^{v+1}$	3^{v+1}	3	$\mathfrak{P}$	3	3^{v+2}	**III**
10	2^{3v+3}	1	1	2^{v+1}	$\mathfrak{P}^{v+1}$	2^{v+1}	2^{v+1}	
	9	10		11	12		13	

I—Nicht–Diskriminantenteiler
II—Reguläre Diskriminantenteiler
III—Irreguläre Diskriminantenteiler

VI, 14

$$\mathfrak{S} \geqq \mathfrak{G} \geqq \mathfrak{G}_Z \geqq \mathfrak{G}_T \geqq \mathfrak{G}_{V_1} \geqq \cdots \geqq \mathfrak{G}V_v \geqq \mathfrak{G}_{V_{v+1}} = \mathfrak{E}\,;$$
$$\mathfrak{G}_{V_v} > \mathfrak{E}\,, \quad \text{wenn} \quad v > 0\,,$$

die den Bedingungen genügen:

$$\mathfrak{G}_T \text{ und die } \mathfrak{G}_{V_n} \text{ sind Normalteiler von } \mathfrak{G}_Z$$
$$\mathfrak{G}_Z/\mathfrak{G}_T \text{ ist zyklisch,} \quad \mathfrak{G}_T/\mathfrak{G}_{V_1} \text{ ist zyklisch,}$$
$$\text{die } \mathfrak{G}_{V_n}/\mathfrak{G}_{V_{n+1}} \text{ sind Abelsch.}$$

In den weiteren Spalten ist dann in leicht verständlicher Weise tabelliert, welche Form die Zerlegung einer Primzahl p aus $\underline{k}$ in $\overline{K}, k, K$ hat, welche Bedingungen für p und seine Primfaktoren $\mathfrak{p}$ in k sich ergeben, und welche Beiträge p zu $\overline{D}, \mathfrak{f}, d, \mathfrak{F}, D$ liefert, wenn die Hilbertsche Untergruppenreihe eines Primteilers von p in $\overline{K}$ die in Spalte 1 aufgeführte Form hat. Für diesen Zweck brauchte in

Spalte 1 von verschiedenen, zu einander konjugierten Untergruppenreihen immer nur eine als Repräsentant berücksichtigt zu werden. Die *ihr* entsprechenden Primteiler von p in $\overline{K}, k, K$ sind mit $\overline{\mathfrak{P}}, \mathfrak{p}, \mathfrak{P}$ *ohne* Index bezeichnet.

Es ergeben sich alle in den weiteren Spalten aufgeführten Tatsachen als Folgen aus den Elementen der Klassenkörpertheorie (mein Bericht I a, §§ 8,9), bis auf die folgenden Ausnahmen:

1.) Spalte 5, Zeile 5. Hier folgt so nur „$p \neq 3$", nicht „$p \equiv -1$ (3)"

2.) Spalte 8, Zeile 9. Hier folgt so nur „$v = 1, 2, 3$", nicht „$v \neq 2$" und „$v = 1$ für $3|d$ und $\frac{d}{3} \equiv 1(3)$."

VI, 15

Die drei Ergänzungen: „$p \equiv 1$ (3)", „$v \neq 2$", „$v = 1$ für $3|d$ und $\frac{d}{3} \equiv 1$ (3)" ergeben sich, wenn man beachtet, daß $\mathfrak{f}$ der *genaue* Führer von H ist. Daß „$v \neq 2$" ist, folgt übrigens auch schon, nach Vollendung der Tabelle, aus $D = df^2$.

Aus der Tabelle folgt die wichtige Tatsache:

$$\mathfrak{f} = f.$$

Wenn man demnach d und H als *klassenkörpertheoretische Invarianten* des kubischen Körpers K betrachtet, so bestimmt sich aus ihnen die Diskriminante D von K als

$$D = df^2,$$

wo f der Führer von H ist. Und umgekehrt sind d und f durch D bestimmt, d. h. die Vorgabe der Diskriminante eines kubischen Körpers K ist gleichwertig mit der Vorgabe der Invariante d und statt der Invariante H nur ihres Führers f.

Durch die Invarianten d, H bestimmt sich nach der Tabelle das *Zerlegungsgesetz* in K (und auch in $\overline{K}$) folgendermaßen:

Geht p nicht in D auf, so liegt Zeile 1, 2 oder Zeile 3 vor, je nachdem $\left(\frac{d}{p}\right) = +1$ oder $\left(\frac{d}{p}\right) = -1$ ist; und im ersten Falle Zeile 1 oder Zeile 2, je nachdem die beiden Primfaktoren $\mathfrak{p}, \mathfrak{p}'$ von p in k zu H gehören oder nicht.

Geht $p \neq 2, 3$ in D auf, so liegt Zeile 4 oder Zeile 5 oder Zeile 6 vor, je nachdem $\left(\frac{d}{p}\right) = +1$ oder $\left(\frac{d}{p}\right) = -1$ oder $\left(\frac{d}{p}\right) = 0$ ist.

Geht $p = 2$ in D auf, so liegt Zeile 5 oder Zeile 10 vor, je nachdem $\left(\frac{d}{2}\right) = -1$ oder $\left(\frac{d}{2}\right) = 0$ ist.

Geht $p = 3$ in D auf, so liegt Zeile 6 oder Zeile 7, 8, 9 vor, je nachdem 3 in f nicht aufgeht oder aufgeht (d. i. auch: je nachdem 3 in D nur zur ersten Potenz oder zu einer höheren aufgeht); und im letzten Falle Zeile 7 oder Zeile 8 oder Zeile 9, je nachdem $\left(\frac{d}{3}\right) = +1$ oder $\left(\frac{d}{3}\right) = -1$ oder $\left(\frac{d}{3}\right) = 0$ ist.

VI, 16

Das Zerlegungsgesetz ist, bis auf die Unterscheidung von Zeile 1 und Zeile 2, allein durch d und f, d. h. *allein durch die Diskriminante D von K* bestimmt. Nur für jene Unterscheidung braucht man H heranzuziehen.

Auf Grund des in der folgenden Eintragung] bewiesenen Satzes folgt sofort, daß H eine solche Idealgruppe mod. f ist, die alle rationalen Zahlen enthält, also eine *Gruppe von Ringklassen* mod. f*, deren Führer f ist*, und daß umgekehrt jeder solchen Idealgruppe mod. f vom Index 3 ein kubischer Körper K der Diskriminante $D = df^2$ entspricht. Daraus bestimmt sich die Anzahl der kubischen Körper vorgegebener Diskriminante $D = df^2$.

Um sie genau zu bestimmen, wähle man in $k = \underline{k}(\sqrt{d})$ zunächst eine zu $\mathfrak{f}$ prime Basis $\mathfrak{r}_1, \ldots, \mathfrak{r}_t$ für die absoluten Idealklassen, deren Ordnungen 3–Potenzen sind. Man beachte ferner, daß f die Gestalt haben muß:

$$f = p_1 \cdots p_n 3^{w\mathfrak{o}} \qquad \mathfrak{o} = 0 \text{ oder } 1, \quad n \geqq 0$$

VI, 17 wo die Primzahlen

$$p_i \equiv \left(\frac{d}{p_i}\right) \text{ mod. } 3$$

sind und

$$w = \begin{cases} 2 & \text{für} \quad 3 \nmid d \\ 1 \text{ oder } 2 & \text{für} \quad 3|d\,, \quad \frac{d}{3} \equiv -1 \ (3) \\ 1 & \text{für} \quad 3|d\,, \quad \frac{d}{3} \equiv 1 \ (3). \end{cases}$$

Man wähle dann je eine primitive Wurzel ϱ_i für den bezw. einen Primteiler von p_i in k und mache zudem

$$\varrho_i \equiv 1 \text{ mod. } \frac{f}{\mathfrak{p}_i}\,.$$

Für den Faktor 3^w wähle man entsprechend den genannten drei Fällen:

a.) $3 \nmid d$ eine Zahl ϱ_0, sodaß jede zu 3 prime Zahl α in der Form

$$\alpha \equiv \varrho_0^a \gamma^3 r \text{ mod. } 3^2 \quad (r \text{ rat.})$$

darstellbar ist, und zudem

$$\varrho_0 \equiv 1 \text{ mod. } \frac{f}{3^2}$$

b.) $3|d$, $\frac{d}{3} \equiv -1$

$$\varrho_0 \equiv 1 + \sqrt{d}\,, \quad \overline{\varrho}_0 \equiv 1 + 3\sqrt{d} \mod 3^2$$

$$\varrho_0, \overline{\varrho}_0 \equiv 1 \mod \frac{f}{3^2} \quad \left(\begin{array}{c} \text{Falls } w = 1 \\ \text{nehme man} \\ \text{den Fall c.)} \end{array} \right)$$

c.) $3|d$, $\frac{d}{3} \equiv 1$ (3) nur das eben genannte ϱ_0.

VI, 18

Dann besitzt jedes zu f prime Ideal $\mathfrak{a}$ aus k eine Darstellung

$$\mathfrak{a} = \mathfrak{r}_1^{x_1} \cdots \mathfrak{r}_t^{x_t} \varrho_1^{y_1} \cdots \varrho_n^{y_n} \begin{bmatrix} \varrho_0^{y_0} \\ \varrho_0^{y_0} \overline{\varrho}_0^{\overline{y}_0} \end{bmatrix}^0 \cdot c^3 \cdot r \cdot \gamma$$

$$\left(\begin{array}{c} r \quad \text{rational} \\ \gamma \equiv 1 \mod f \end{array} \right)$$

In dieser sind die x_i mod. 3 eindeutig, die y_i dagegen nicht notwendig, wegen der von den 3–ten Idealpotenzzahlen

$$\varepsilon_k = \varrho_1^{y_{1k}} \cdots \varrho_n^{y_{nk}} \begin{bmatrix} \varrho_0^{y_{0k}} \\ \varrho_0^{y_{0k}} \overline{\varrho}_0^{\overline{y}_{0k}} \end{bmatrix}^0 \alpha^3 \cdot r \cdot \gamma\,, \qquad \begin{array}{l} (k = t + t_0) \\ (t_0 = 0 \text{ oder } 1) \end{array}$$

herrührenden Relationen. Es darf nämlich eine beliebige Linearkombination der y_{ik} zu den y_i hinzugefügt werden.

Jede der gesuchten Idealgruppen wird nun durch eine lineare Kongruenz

$$L(x_i, y_i) \equiv 0 \mod 3$$

definiert, d. h. $\mathfrak{a}$ gehört zu H, wenn seine Exponenten dieser Kongruenz genügen. Nicht proportionalen L entsprechen verschiedene H. Sei

$$L(x_i, y_i) = \sum_i X_i x_i + \sum_i Y_i y_i\,.$$

Damit L wirklich eine *Ideal*gruppe definiert, muß L für die ε_k identisch verschwinden, d. h.

$$L(0, y_{ik}) = \sum_i Y_i y_{ik} \equiv 0 \mod 3$$

sein für alle k. Und damit H wirklich den *Führer* f bekommt, müssen die $Y_i \not\equiv 0$ mod. 3 sein (bis auf Y_0, sofern $\overline{Y}_0$ vorhanden, d. h. $w = 2$).

VI, 19

Daraus ergibt sich dann durch Abzählung die Anzahl der kubischen Körper mit der Diskriminante $D = df^2$.

6.6 Eine Frage aus Artin's Reziprozitätsgesetz. (Okt.1928)

Hasse investigates how to decide from the class group whether an abelian extension $L|K$ is abelian over a subfield k (or at least galois), where $K|k$ is cyclic. The corresponding group theoretic question was covered in the entry of October 3.] The special case of cubic class fields over a quadratic field has occurred in the foregoing entry.] Later in 1929 Hasse included the content of the present entry in his class field report [Has30c]. *Still later, Hasse studied extensively similar problems on the basis of Kummer theory instead of class field theory, and also in more general settings. See, e.g.,* [Has49]

VI, 20

(Oktober 1928)

Satz. *Es sei*

k_0 *ein algebraischer Zahlkörper*

k *ein über k_0 zyklischer Zahlkörper*

τ *eine erzeugende Substitution von K/k_0*

K *ein über k Abelscher Zahlkörper*

H *die Idealgruppe in k, zu der K Klassenkörper ist*

Dann und nur dann ist K Abelsch über k_0, wenn die Klassen nach H bei τ invariant sind.

Beweis: a.) Damit K/k_0 Abelsch ist, muß K/k_0 jedenfalls Galoissch sein. Dafür ist notwendig und hinreichend, daß H bei τ invariant ist.

b.) Es sei also H bei τ invariant, somit K/k_0 Galoissch. Es bezeichne dann

$\overline{\mathfrak{G}}$ die Galoissche Gruppe von K/k_0

$\mathfrak{G}$ die Galoissche Gruppe von K/k

$\overline{\mathfrak{G}}/\mathfrak{G}$ ist zur zyklischen Gruppe $\{\tau\}$ isomorph. Dieser Isomorphismus kann dargestellt werden, indem einer Nebenschar aus $\overline{\mathfrak{G}}/\mathfrak{G}$ die durch ihre Substitutionen bewirkte Substitution für die Zahlen aus k zugeordnet wird. Auf diese

VI, 21

Weise entspreche die Erzeugende τ der Nebenschar $\overline{\tau}\mathfrak{G}$. Dann ist $\overline{\mathfrak{G}}/\mathfrak{G} = \{\overline{\tau}\mathfrak{G}\}$. K/k_0 ist Abelsch dann und nur dann, wenn $\overline{\mathfrak{G}}$ Abelsch ist, d. h. wenn

$$\overline{\tau}\sigma\overline{\tau}^{-1} = \sigma$$

für jede Substitution σ aus $\mathfrak{G}$ ist.

Nach dem Isomorphiesatz der Klassenkörpertheorie ist $\mathfrak{G}$ isomorph zur Gruppe der Klassen nach H. Und nach dem Artinschen Reziprozitätsgesetz kann dieser Isomorphismus dargestellt werden, indem einer Klasse C nach H diejenige Substitution σ aus $\mathfrak{G}$ zugeordnet wird, die für jedes Primideal $\mathfrak{p}$ aus C die Relation

$$\mathsf{A}^{N(\mathfrak{p})} \equiv \sigma\mathsf{A} \ \text{mod.}\, \mathfrak{p}$$

für alle ganzen Zahlen A aus $\overline{K}$ befriedigt. Weil aus dieser Relation folgt

$$(\overline{\tau}\mathsf{A})^{N(\mathfrak{p})} \equiv \overline{\tau}\sigma\overline{\tau}^{-1}(\overline{\tau}\mathsf{A}) \ \text{mod.}\, \overline{\tau}\mathfrak{p}\,,$$

so ist der Klasse $\overline{\tau}C = \tau C$ auf dieselbe Weise die Substitution $\overline{\tau}\sigma\overline{\tau}^{-1}$ zugeordnet. Wegen der Eineindeutigkeit der Zuordnung ist also dann und nur dann $\overline{\tau}\sigma\overline{\tau}^{-1} = \sigma$ für jede Substitution σ aus $\mathfrak{G}$, wenn $\tau C = C$ für jede Klasse C nach H ist.

6.7 Zur Hauptidealisierung in Unterkörpern des ℓ–Klassenkörpers bei imaginär–quadratischem Grundkörper. (Dez.1928)

Furtwängler's proof of the principal ideal theorem of class field theory was already known to Hasse when he wrote down this note; see [FR08]*. Here Hasse studies the capitulation of ideals in an unramified cyclic extension $K|k$ of odd prime power degree ℓ^n. The base field k is supposed to be imaginary quadratic. Hasse shows that there are precisely ℓ^n ideal classes which capitulate in K. In the case $n = 1$ this had been proved by Arnold Scholz whose proof was known to Hasse. The theorem was later included in Hasse's class field report* [Has30b].

VI, 22

(Dezember 1928)

Sei k ein imaginär–quadratischer Grundkörper und ℓ eine ungerade Primzahl. In k sei die Einteilung in die absoluten „ℓ–Klassen" zugrundegelegt, also alle und nur die absoluten Idealklassen von zu ℓ primer Ordnung in die Hauptklasse gerechnet. Es sei K der zugehörige Klassenkörper, der absolute „ℓ–Klassenkörper" zu k.

Satz. *Es sei K_0 ein relativ–zyklischer Teilkörper über k des absoluten ℓ–Klassenkörpers K zu k, vom Relativgrade ℓ^n. In K_0 wird genau eine Untergruppe der Ordnung ℓ^n der absoluten ℓ–Klassengruppe von k ℓ–hauptidealisiert.*

Beweis: Die ℓ–Klassen aus k liefern ambige ℓ–Klassen aus K_0, d. h. bei der Substitution S_0 von K_0 (und ihren Potenzen) invariant. Nach der Geschlechtertheorie der allgemeinen Klassenkörpertheorie hat die Gruppe der ambigen ℓ–Klassen in K_0 genau den ℓ^n–ten Teil der ℓ–Klassenzahl in k zur Ordnung. Der Satz wird also bewiesen sein, wenn gezeigt ist, daß auch umgekehrt jede ambige ℓ–Klasse aus K_0 durch eine ℓ–Klasse aus k geliefert wird.

VI, 23

Sei nun C eine ambige ℓ–Klasse aus K_0. Für ein Ideal $\mathfrak{A}$ aus C gilt dann

$$\mathfrak{A}^{1-\mathsf{S}_0} \sim 1,$$

d. h. es gibt ein zu ℓ primes q mit

$$\mathfrak{A}^{q(1-\mathsf{S}_0)} = (\mathsf{A}).$$

Daraus folgt für die Relativnorm

$$N(\mathsf{A}) = \pm 1\,,$$

weil in k keine anderen Einheiten enthalten sind. Da ℓ ungerade, kann ohne Einschränkung

$$N(\mathsf{A}) = 1$$

angenommen werden; denn $N(-1) = -1$. Dann ist aber

$$\mathsf{A} = \mathsf{B}^{1-\mathsf{S}_0}.$$

Also

$$\left(\frac{\mathfrak{A}^q}{(\mathsf{B})}\right)^{1-\mathsf{S}_0} = 1.$$

Da K_0 über k unverzweigt ist, sind bei S_0 invariant allein die Ideale aus k. Daher gilt:

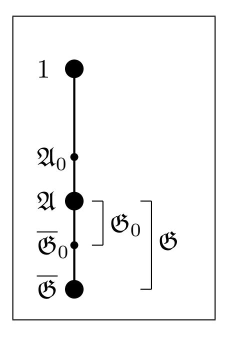
VI, 24

$$\mathfrak{A}^q = (\mathsf{B})\mathfrak{a} \qquad \text{mit } \mathfrak{a} \text{ aus } k.$$

Hiernach wird C^q durch ein Ideal aus k geliefert, also auch C selbst, w. z. b. w.

Es sei jetzt $\mathfrak{G}$ die Galoissche Gruppe von K/k. Den über k relativ–zyklischen Teilkörpern K_0 von K entsprechen dann die Untergruppen $\mathfrak{G}_0$ von $\mathfrak{G}$ mit zyklischen Faktorgruppen.

Um die Hauptidealisierung gruppentheoretisch darzustellen, sei $\overline{\mathfrak{G}}$ die Galoissche Gruppe des zweiten ℓ–Klassenkörpers $\overline{K}/k$, und $\mathfrak{A}$ die von $\overline{K}/K$, also $\overline{\mathfrak{G}}/\mathfrak{A} \cong \mathfrak{G}$. Es ist dann $\mathfrak{A}$ die Kommutatorgruppe von $\overline{\mathfrak{G}}$. Den Untergruppen $\mathfrak{G}_0$ von $\mathfrak{G}$ entsprechen eineindeutig die Gruppen $\overline{\mathfrak{G}}_0$ zwischen $\mathfrak{A}$ und $\overline{\mathfrak{G}}$. Es sei $\mathfrak{A}_0$ die Kommutatorgruppe von $\overline{\mathfrak{G}}_0$, also eine gewisse Untergruppe von $\mathfrak{A}$. Die ℓ–Klassen von k entsprechen dann isomorph den Elementen von $\mathfrak{G} \cong \overline{\mathfrak{G}}/\mathfrak{A}$, und die ℓ–Klassen von K_0 den Elementen von $\overline{\mathfrak{G}}_0/\mathfrak{A}_0$. Ist $\mathfrak{G}/\mathfrak{G}_0$, wie vorausgesetzt, zyklisch, also auch $\overline{\mathfrak{G}}/\overline{\mathfrak{G}}_0$ zyklisch,



VI, 25

so sei

$$\overline{\mathfrak{G}} = \left\{ \mathsf{S}_0, \overline{\mathfrak{G}}_0 \right\} .$$

Die ℓ–Klassen in k, die den kleinsten $\mathsf{S}\mathfrak{A}$ aus $\mathfrak{G}_0 \cong \overline{\mathfrak{G}}_0/\mathfrak{A}$ entsprechen, kurz „die ℓ–Klassen S“, enthalten die in K_0 voll zerfallenden Primideale aus k. Diese Klassen gehören in K_0 zu den Elementen

$$\mathsf{S}^{1+\mathsf{S}_0+\cdots+\mathsf{S}_0^{\ell^n-1}}\mathfrak{A}_0$$

von $\overline{\mathfrak{G}}_0/\mathfrak{A}_0$. Die ℓ–Klasse S_0 von k enthält die in K_0 unzerlegten Primideale aus k. Sie gehört in K_0 zu

$$\mathsf{S}_0^{\ell^n}\mathfrak{A}_0.$$

Allgemein gehört die ℓ–Klasse $\mathsf{S}^{\nu_0}\mathsf{S}$ von k daher in K_0 zur ℓ–Klasse

$$\mathsf{S}_0^{\nu_0\ell^n}\mathsf{S}^{1+\mathsf{S}_0+\cdots+\mathsf{S}_0^{\ell^n-1}}\mathfrak{A}_0.$$

Die $\mathsf{S}_0^{\nu_0}\mathsf{S}$, für die diese ℓ–Klasse die Einheit $\mathfrak{A}_0$ ist, müssen nun nach dem obigen Satz eine Gruppe genau von der Ordnung ℓ^n bilden. Jeder Untergruppe $\mathfrak{G}_0$ von $\mathfrak{G}$, mit zyklischer Faktorgruppe der Ordnung ℓ^n, ist so eine bestimmte Untergruppe der Ordnung ℓ^n von $\mathfrak{G}$ (nicht notwendig zyklisch) zugeordnet.

VI, 26

Ich studiere diese Zuordnung näher für die einfachsten Fälle, die $\mathfrak{G}$ darbieten kann.

Ist zunächst $\mathfrak{G}$ selbst zyklisch, so ist

$$\overline{\mathfrak{G}} = \{\mathsf{S}, \mathfrak{A}\} .$$

Da aber $\mathfrak{A}$ die Kommutatorgruppe von $\overline{\mathfrak{G}}$ sein soll, muß $\mathfrak{A} = 1$ sein; siehe die Furtwänglersche Arbeit zum Hauptidealsatz. Es gilt also:

Satz. *Ist die ℓ–Klassengruppe von k zyklisch, so ist die ℓ–Klassengruppe von K die Einheit.*

Es sei jetzt

$$\overline{\mathfrak{G}} = \{\mathsf{S}_1, \mathsf{S}_2, \mathfrak{A}\}$$

und zwar $\mathfrak{G} \cong \overline{\mathfrak{G}}/\mathfrak{A}$ vom Typus (ℓ, ℓ). Wird

$$\mathsf{S}_2^{-1}\mathsf{S}_1^{-1}\mathsf{S}_2\mathsf{S}_1 = A \qquad \text{(aus } \mathfrak{A})$$

gesetzt, so besteht (nach der genannten Furtwänglerschen Arbeit) $\mathfrak{A}$ aus der Gesamtheit der symbolischen Potenzen $A^{F(\mathsf{S}_1,\mathsf{S}_2)}$. Es sei insbesondere

$$\mathsf{S}_1^\ell = A^{F_1(\mathsf{S}_1,\mathsf{S}_2)}\,, \quad \mathsf{S}_2^\ell = A^{F_2(\mathsf{S}_1,\mathsf{S}_2)}$$

Nach Schreier, Gruppenerweiterung, genügen dann $\mathsf{S}_1, \mathsf{S}_2$ und F_1, F_2 den symbolischen Kongruenzen: VI, 27

$$\begin{gathered}
\mathsf{S}_1^\ell \equiv 1\,, \quad \mathsf{S}_2^\ell \equiv 1 \\
\mathsf{S}_1\mathsf{S}_2 \equiv \mathsf{S}_2\mathsf{S}_1 \\
(\mathsf{S}_1 - 1)F_1 \equiv 0\,, \quad (\mathsf{S}_2 - 1)F_2 \equiv 0 \\
(\mathsf{S}_1 - 1)F_2 \equiv 1 + \mathsf{S}_2 + \cdots + \mathsf{S}_2^{\ell-1}, \quad -(\mathsf{S}_2 - 1)F_1 \equiv 1 + \mathsf{S}_1 + \cdots + \mathsf{S}_1^{\ell-1},
\end{gathered}$$

deren Sinn ist, daß im Exponenten von A nach ihnen gerechnet werden darf.

Die Untergruppen von $\mathfrak{G}$ mit zyklischer Faktorgruppe werden jetzt selbst zyklisch von der Ordnung ℓ und durch Angabe eines erzeugenden Elements $\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2}$ bestimmt, bei dem es natürlich für (μ_1, μ_2) nur bis auf mod. ℓ proportionale Systeme ankommt. Entsprechend werden die Untergruppen der Ordnung ℓ, die den eben genannten durch die Hauptidealisierung zugeordnet sind, durch $\mathsf{S}_1^{\nu_1}\mathsf{S}_2^{\nu_2}$ mit ähnlich bestimmten (ν_1, ν_2) repräsentiert. Jedem (μ_1, μ_2) ist dann also eindeutig ein (ν_1, ν_2) zugeordnet durch die Beziehung, daß im Körper zu $\{\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2}\}$ die Klassen zu $\{\mathsf{S}_1^{\nu_1}\mathsf{S}_2^{\nu_2}\}$ hauptidealisiert werden. VI, 28

Sind μ_1 und μ_2 beide $\not\equiv 0$ mod. ℓ, so entsprechen im Körper zu $\{\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2}\}$ den Klassen S_1 und S_2 die Klassen

$$\mathsf{S}_1^\ell = A^{F_1(\mathsf{S}_1,\mathsf{S}_2)}, \qquad \mathsf{S}_2^\ell = A^{F_2(\mathsf{S}_1,\mathsf{S}_2)},$$

also der Klasse $\mathsf{S}_1^{\nu_1}\mathsf{S}_2^{\nu_2}$ die Klasse

$$A^{\nu_1 F_1(\mathsf{S}_1,\mathsf{S}_2) + \nu_2 F_2(\mathsf{S}_1,\mathsf{S}_2)}.$$

Ist $\mu_1 \equiv 0$ mod. ℓ, also $\mu_2 \not\equiv 0$ mod. ℓ, so entspricht der Klasse S_1 wieder die Klasse

$$\mathsf{S}_1^\ell = A^{F_1(\mathsf{S}_1,\mathsf{S}_2)},$$

der Klasse S_2 dagegen die Klasse

$$\mathsf{S}_2^{1+\mathsf{S}_1+\cdots+\mathsf{S}_1^{\ell-1}} = \prod_{k=0}^{\ell-1} \mathsf{S}_1^{-k}\mathsf{S}_2\mathsf{S}_1^k$$

Nun ist allgemein

$$\mathsf{S}_2^{\nu_2}\mathsf{S}_1^{\nu_1} = \mathsf{S}_1^{\nu_1}\mathsf{S}_2^{\nu_2} A^{\frac{\mathsf{S}_1^{\nu_1}-1}{\mathsf{S}_1-1}\,\frac{\mathsf{S}_2^{\nu_2}-1}{\mathsf{S}_2-1}},$$

also speziell

$$\mathsf{S}_1^{-k}\mathsf{S}_2\mathsf{S}_1^{k} = \mathsf{S}_2 A^{\frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}}$$

$$\begin{aligned} \mathsf{S}_2^{1+\mathsf{S}_1+\cdots+\mathsf{S}_1^{\ell-1}} &= \prod_{k=0}^{\ell-1} \mathsf{S}_2 A^{\frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}} = \mathsf{S}_2^{\ell} A^{\sum\limits_{k=0}^{\ell-1} \mathsf{S}_2^{\ell-1-k}\frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}} \\ &= A^{F_2(\mathsf{S}_1,\mathsf{S}_2)+\sum\limits_{k=0}^{\ell-1} \mathsf{S}_2^{\ell-1-k}\frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}} \\ &\sim A^{F_2(\mathsf{S}_1,\mathsf{S}_2)+\sum\limits_{k=0}^{\ell-1} \frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}} \end{aligned}$$

VI, 29 letzteres für die zu $\left\{\mathsf{S}_1^0\mathsf{S}_2^{\mu_2}, \mathfrak{A}\right\} = \{\mathsf{S}_2, \mathfrak{A}\}$ gehörige Kommutatorgruppe, d. h. $\mathsf{S}_2 \equiv 1$ im Exponenten von A. Ist $\mu_1 \not\equiv 0$ mod. ℓ, $\mu_2 \equiv 0$ mod. ℓ, so folgt analog, daß der Klasse S_2 die Klasse

$$\mathsf{S}_2^{\ell} = A^{F(\mathsf{S}_1,\mathsf{S}_2)}$$

und der Klasse S_1 die Klasse

$$\mathsf{S}_1^{1+\mathsf{S}_2+\cdots+\mathsf{S}_2^{\ell-1}} \sim A^{F_1(\mathsf{S}_1,\mathsf{S}_2)-\sum\limits_{k=0}^{\ell-1}\frac{\mathsf{S}_2^{k}-1}{\mathsf{S}_2-1}}$$

entspricht.

Alles zusammengefaßt ergibt sich, daß die Klasse $\mathsf{S}_1^{\nu_1}\mathsf{S}_2^{\nu_2}$ aus k im Körper zu $\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2}$ übergeht in die Klasse

$$A^{\nu_1\left(F_1(\mathsf{S}_1,\mathsf{S}_2)-\delta_{0\mu_2}\sum\limits_{k=0}^{\ell-1}\frac{\mathsf{S}_2^{k}-1}{\mathsf{S}_2-1}\right)+\nu_2\left(F_2(\mathsf{S}_1,\mathsf{S}_2)+\delta_{0\mu_1}\sum\limits_{k=0}^{\ell-1}\frac{\mathsf{S}_1^{k}-1}{\mathsf{S}_1-1}\right)},$$

wobei

$$\delta_{ij} = \left\{ \begin{array}{lll} 1 & \text{für} & j \equiv i\ (\ell) \\ 0 & \text{"} & j \not\equiv i\ (\ell) \end{array} \right\}.$$

Hierbei kann im Exponenten von A nach der Vorschrift

$$\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2} \equiv 1$$

gerechnet werden.

Faßt man alle Rechenvorschriften zusammen, die für den Exponenten von A bestehen, so ergibt sich ein bestimmtes Ideal, sodaß $A^{F(\mathsf{S}_1,\mathsf{S}_2)}$ dann und nur dann 1 ist, wenn $F(\mathsf{S}_1,\mathsf{S}_2)$ zu diesem Ideal gehört. Für dieses Ideal gelten jedenfalls die bisher gegebenen Kongruenzen, ev. aber noch mehr. Für jedes $\mathsf{S}_1^{\mu_1}\mathsf{S}_2^{\mu_2}$ resultiert natürlich ein besonderes Ideal. VI, 30

Diese Ideale lassen sich als bestimmte Ideale des Körpers der ℓ–ten Einheitswurzeln realisieren, wenn man

$$\mathsf{S}_1 = \zeta^{-\mu_2}, \qquad \mathsf{S}_2 = \zeta^{\mu_1}$$

setzt. Dann entsteht (weil $\mathfrak{A}$ eine ℓ–Gruppe) ein Ideal der Form $\lambda^{m_{\mu_1,\mu_2}+1}$, wo $\lambda = 1-\zeta$. Nach obigem Satz ist es dadurch eindeutig bestimmt, daß der zuletzt bestimmte Exponent von A genau für eine Untergruppe der Ordnung ℓ aller (ν_1,ν_2), d. h. genau für ein System zueinander proportionaler (ν_1,ν_2) kongruent Null nach ihm sein muß. $\lambda^{m_{\mu_1,\mu_2}}$ ist also der größte gemeinsame Teiler der Faktoren von ν_1 und ν_2 in jenem Exponenten, wenn

$$\mathsf{S}_1 = \zeta^{-\mu_2}, \qquad \mathsf{S}_2 = \zeta^{\mu_1}$$

gesetzt wird.Die Richtigkeit dieser Tatsache ergibt sich daraus, daß nach den Relationen a. S. 27] oben auf alle Fälle die λ–fachen der Faktoren von ν_1 und ν_2 in jenem Exponenten $\equiv 0$ nach dem Ideal des Kreiskörpers $\lambda^{m_{\mu_1,\mu_2}+1}$ sind. VI, 31

Man kann jene Exponenten wegen

$$\delta_{ij} = \frac{\sum_{k=0}^{\ell-1}\zeta^{(i-j)k}}{\ell} = \frac{1}{\ell}\,\frac{\zeta^{(i-j)\ell}-1}{\zeta-1}$$

auch so erhalten:

$$\begin{aligned} G_1(\mathsf{S}_1,\mathsf{S}_2) &= F_1(\mathsf{S}_1,\mathsf{S}_2) - \frac{1}{\ell}\,\frac{\mathsf{S}_1^\ell-1}{\mathsf{S}_1-1}\sum_{k=0}^{\ell-1}\frac{\mathsf{S}_2^k-1}{\mathsf{S}_2-1} \\ G_2(\mathsf{S}_1,\mathsf{S}_2) &= F_2(\mathsf{S}_1,\mathsf{S}_2) - \frac{1}{\ell}\,\frac{\mathsf{S}_2^\ell-1}{\mathsf{S}_2-1}\sum_{k=0}^{\ell-1}\frac{\mathsf{S}_1^k-1}{\mathsf{S}_1-1}\,. \end{aligned}$$

Das sind gebrochene Polynome in $\mathsf{S}_1,\mathsf{S}_2$, die aber bei obiger Realisierung

$$\mathsf{S}_1 = \zeta^{-\mu_2}, \qquad \mathsf{S}_2 = \zeta^{\mu_1}$$

in ganze Zahlen des Kreiskörpers, nämlich gerade in die gesuchten Exponenten übergehen. Wird dementsprechend

$$\begin{aligned} G_1(\zeta^{-\mu_2}, \zeta^{\mu_1}) &\equiv a_1^{(\mu_1,\mu_2)} \lambda^{m_{\mu_1,\mu_2}} \mod \lambda^{m_{\mu_1,\mu_2}+1} \\ G_2(\zeta^{-\mu_2}, \zeta^{\mu_1}) &\equiv a_2^{(\mu_1,\mu_2)} \lambda^{m_{\mu_1,\mu_2}} \mod \lambda^{m_{\mu_1,\mu_2}+1} \end{aligned}$$

VI, 32 gesetzt, so bestimmen sich die gesuchten ν_1, ν_2 aus μ_1, μ_2 durch die lineare Kongruenz

$$\nu_1 a_1^{(\mu_1,\mu_2)} + \nu_2 a_2^{(\mu_1,\mu_2)} \equiv 0 \text{ mod. } \ell.$$

Der einfachste Typus liegt vor, wenn $F_1(\mathsf{S}_1, \mathsf{S}_2)$ und $F_2(\mathsf{S}_1, \mathsf{S}_2)$, nach Potenzen von

$$\Delta_1 = 1 - \mathsf{S}_1, \qquad \Delta_2 = 1 - \mathsf{S}_2$$

entwickelt, nicht beide mod. ℓ verschwindende Anfangsglieder haben. Sei also:

$$\begin{gathered} F_1(\mathsf{S}_1, \mathsf{S}_2) \equiv a_1 \text{ mod. } (\Delta_1, \Delta_2) \\ F_2(\mathsf{S}_1, \mathsf{S}_2) \equiv a_2 \text{ mod. } (\Delta_1, \Delta_2) \\ (a_1, a_2, \ell) = 1. \end{gathered}$$

Faßt man $F_1(\mathsf{S}_1, \mathsf{S}_2)$ und $F_2(\mathsf{S}_1, \mathsf{S}_2)$ als Potenzreihen mit Koeffizienten aus dem ℓ–adischen Zahlkörper auf, so besitzt daher mindestens einer ein Reziprokes. Mit diesem darf im Exponenten von A gerechnet werden, weil A^{ℓ^N} und

VI, 33 $A^{(1-\mathsf{S}_1)^N}, A^{(1-\mathsf{S}_2)^N}$ für hinreichend hohes N gleich 1 sind ($\mathfrak{A}$ ist ℓ–Gruppe). Ist etwa $a_1 \not\equiv 0$ mod. ℓ, sodaß F_1^{-1} existiert, so folgt aus

$$(\mathsf{S}_1 - 1)F_1 \equiv 0, \quad \text{daß} \quad \mathsf{S}_1 - 1 \equiv 0$$

ist, und aus

$$(1 - \mathsf{S}_2)F_1 \equiv 1 + \mathsf{S}_1 + \cdots + \mathsf{S}_1^{\ell-1} \equiv \ell,$$

daß

$$1 - \mathsf{S}_2 \equiv \ell F_1^{-1}$$

ist; schließlich ist

$$1 + \mathsf{S}_2 + \cdots + \mathsf{S}_2^{\ell-1} \equiv (\mathsf{S}_1 - 1)F_2 \equiv 0,$$

also

$$\ell + \binom{\ell}{2}\Delta_2 + \cdots + \binom{\ell}{\ell-1}\Delta_2^{\ell-2} + \Delta_2^{\ell-1} \equiv 0,$$

$$\ell + \binom{\ell}{2}\ell F_1^{-1} + \cdots + \binom{\ell}{\ell-1}\ell^{\ell-2}(F_1^{-1})^{\ell-2} + \ell^{\ell-1}(F_1^{-1})^{\ell-1} \equiv 0$$

Da nun

$$1 + \binom{\ell}{2}F_1^{-1} + \cdots + \binom{\ell}{\ell-1}\ell^{\ell-3}(F_1^{-1})^{\ell-2} + \ell^{\ell-2}(F_1^{-1})^{\ell-1}$$

ein Reziprokes besitzt, muß

$$\ell \equiv 0$$

sein, daher schließlich auch

$$\mathsf{S}_2 - 1 \equiv 0.$$

Hiernach ist $\mathfrak{A} = \{A\}$ zyklisch von der Ordnung ℓ ($\mathfrak{A} = 1$ ist mit der Voraussetzung nicht vereinbar), und die gesuchten ν_1, ν_2 bestimmen sich für alle μ_1, μ_2 aus ein– u. derselben Kongruenz VI, 34

$$\nu_1 a_1 + \nu_2 a_2 \equiv 0 \mod \ell.$$

Der nächst einfachere Typus ist:

$$\begin{aligned} F_1(\mathsf{S}_1, \mathsf{S}_2) &= a_{11}\Delta_1 + a_{12}\Delta_2 + \cdots \\ F_2(\mathsf{S}_1, \mathsf{S}_2) &= a_{21}\Delta_1 + a_{22}\Delta_2 + \cdots \end{aligned}$$

Dabei sei

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \not\equiv 0 \mod \ell.$$

Die Realisierung

$$\mathsf{S}_1 = \zeta^{-\mu_2}, \qquad \mathsf{S}_2 = \zeta^{\mu_1}$$

ergibt

$$\begin{aligned} F_1(\zeta^{-\mu_2}, \zeta^{\mu_1}) &\equiv (-\mu_2 a_{11} + \mu_1 a_{12})\lambda \text{ mod. } \lambda^2 \\ F_2(\zeta^{-\mu_2}, \zeta^{\mu_1}) &\equiv (-\mu_2 a_{21} + \mu_1 a_{22})\lambda \text{ mod. } \lambda^2. \end{aligned}$$

Nach Voraussetzung sind nun jene beiden Koeffizienten rechts nie beide $\equiv 0$ mod. ℓ, wenn (μ_1, μ_2) nicht identisch mod. ℓ verschwindet. Also folgt (für VI, 35 $\ell > 3$, wo die Zusatzglieder fortfallen):

$$m_{\mu_1,\mu_2} = 1 \qquad \text{für alle} \quad \mu_1, \mu_2.$$

Und ν_1, ν_2 bestimmen sich aus

$$\nu_1(-\mu_2 a_{11} + \mu_1 a_{12}) + \nu_2(-\mu_2 a_{21} + \mu_1 a_{22}) \equiv 0 \text{ mod. } \ell,$$

d. h.

$$\left.\begin{aligned} \nu_1 &\equiv \mu_1 a_{22} - \mu_2 a_{21} \\ \nu_2 &\equiv -\mu_1 a_{12} + \mu_2 a_{11} \end{aligned}\right\} \text{ mod. } \ell.$$

Setzt man

$$\mathsf{A} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix},$$

so besteht hiernach zwischen ν_1, ν_2 und μ_1, μ_2 die Beziehung

$$(\mu_1, \mu_2) \equiv \mathsf{A}(\nu_1, \nu_2) \text{ mod. } \ell,$$

da es ja auf Proportionalitätsfaktoren nicht ankommt.

6.8 Der Fundamentalsatz aus der Geschlechtertheorie quadratischer Formen von n Variablen. (Dez.1928)

Genus theory of quadratic forms in n variables.

VI, 36

Dezember 1928

Der Satz lautet:

Quadratische Formen desselben Geschlechts können durch unimodulare für ein beliebiges M ganze Transformationen ineinander übergeführt werden.

Ich beweise diesen Satz im Folgenden für die speziellen Ordnungen

$$\begin{matrix} o_1, \ldots, o_{k-1} \quad \text{ungerade} \\ \sigma_1, \ldots, \sigma_{k-1} = 1 \end{matrix} \quad , \quad \mathfrak{I} = 0$$

(in den Minkowskischen Bezeichnungen).

Zunächst einige Vorbereitungen. Es genügt, den Satz für Multipla M von $o_1 \ldots o_{k-1}$ zu beweisen. M sei durchweg von dieser Beschaffenheit. Eine beliebige Form obiger Ordnung kann dann ganzzahlig unimodular in eine charakteristische Form F für M transformiert werden, d. h. in eine solche, für die die Hauptunterdeterminanten VI, 37

$$A_0, A_1, A_2 o_1, A_3 o_1^2 o_2, \ldots, A_{n-1} o_1^{n-2} \cdots o_{n-2}, A_n o_1^{n-1} \cdots o_{n-1}$$

der 0–ten, 1–ten, ..., n–ten Ordnung auf eine Reihe

$$A_0 = 1, A_1, A_2, \ldots, A_{n-1}, A_n = 1$$

von positiven ganzen Zahlen führen, die zu M und je zu ihren Nachbarn teilerfremd sind. Dabei darf den Zahlen $A_1, \ldots, A_{n-1}$ auch noch jede Kongruenzvorschrift mod. 4 gemacht werden, die bei irgendeinem Hauptrest mod. 4 der Ausgangsform vorkommt. Ist $n \geqq 4$, so kann auf diese Weise, wie ich zeigen werde,

$$A_1 \equiv 1 \text{ mod. } 4, \ldots, A_{n-3} \equiv 1 \text{ mod. } 4$$

erreicht werden. Es genügt dazu zu zeigen, daß für $k \geqq 4$ jeder Hauptrest mod. 4 der obigen Ordnung einem solchen mod. 4 durch unimodulare ganz- VI, 38

zahlige Transformation kongruent–äquivalent ist, der an der ersten Stelle der Hauptdiagonale durch +1 mod. 4 besetzt ist. Dies ist nur für den Hauptrest $\begin{pmatrix} -1 & & & & \\ & -1 & & & \\ & & -1 & & \\ & & & -1 & \\ & & & & \ddots \end{pmatrix}$ mod. 4 nichttrivial. Durch $\begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & & 1 & & \\ 0 & & & 1 & \\ \vdots & & & & \ddots \end{pmatrix}$ geht er in $\begin{pmatrix} 1 & -1 & -1 & 0 & \\ -1 & -1 & & & \\ -1 & & -1 & & \\ 0 & & & -1 & \\ & & & & \ddots \end{pmatrix}$ über. Diese Form ist vermöge $\begin{pmatrix} 1 & 1 & 1 & 0 & \cdots \\ & 1 & & & \\ & & 1 & & \\ & & & 1 & \\ & & & & \ddots \end{pmatrix}$ kongruent–äquivalent zu $\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots \\ 0 & 2 & -1 & 0 & \\ 0 & -1 & 2 & 0 & \\ 0 & 0 & 0 & -1 & \\ \vdots & & & & \ddots \end{pmatrix}$, diese wiederum leicht durch entsprechende Rücktransformation des Abschnittes aus der zweiten, ... Reihe zu

$$\begin{pmatrix} 1 & & & & & \\ & 1 & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & -1 & \\ & & & & & \ddots \end{pmatrix},$$

also in einen Hauptrest der verlangten Beschaffenheit.

Die in der üblichen Weise vollzogene Transformation der charakteristischen VI, 39 Form F auf die Diagonalform:

$$f = A_1 x_1^2 + \frac{A_2}{A_1} o_1 x_2^2 + \cdots + \frac{A_{n-1}}{A_{n-2}} o_1 \cdots o_{n-2} x_{n-1}^2 + \frac{1}{A_{n-1}} o_1 \cdots o_{n-1} x_n^2$$

ist für M ganz. Es genügt also, Formen in dieser „Normalgestalt“ zu betrachten.

Nicht für jedes System ganzer, positiver, zu M und je zu ihren Nachbarn teilerfremder Zahlen

$$A_0 = 1, A_1, \ldots, A_{n-1}, A_n = 1$$

wird die Form f in der genannten Weise aus einer charakteristischen Form F der betrachteten Ordnung entstehen. Eine notwendige Bedingung für dies Faktum ergibt sich aus den bekannten Unterdeterminantenrelationen zu:

$$\left\{\frac{-A_{\nu-1}A_{\nu+1}o_\nu}{A_\nu}\right\} = 1 \qquad (\nu = 1, \dots, n-1). \tag{1}$$

Dabei ist $\left\{\frac{\cdots}{\cdots}\right\}$ zur Abkürzung für das System aller Legendreschen Symbole des „Zählers“ nach den verschiedenen Primfaktoren des „Nenners“ gesetzt. VI, 40

Für $n = 2$ reduziert sich diese Bedingungsserie auf die einzige Bedingung

$$\left\{\frac{-o_1}{A_1}\right\} = 1. \tag{1'}$$

Diese ist nun zugleich hinreichend dafür, daß die binäre Form

$$\varphi = A_1 x_1^2 + \frac{1}{A_1} o_1 x_2^2$$

aus einer charakteristischen Form Φ für M der Ordnung $\left(\begin{array}{c|c} o_1 & \\ 1 & 0 \end{array}\right)$ in obiger Weise entspringt. Nach (1') gibt es nämlich eine Lösung α_0 von

$$\alpha_0^2 + o_1 \equiv 0 \ \text{mod.}\ A_1 \,,$$

etwa

$$\alpha_0^2 + o_1 = A_1 a_0$$

Wird

$$\alpha = \alpha_0 + tA_1$$

und

$$\alpha^2 + o_1 = A_1 a$$

gesetzt, so berechnet sich die ganze Zahl a als

$$a = a_0 + 2t\alpha_0 + t^2 A_1 \,.$$

VI, 41 Jetzt kann durch passende Wahl von t erreicht werden, daß a prim zu M ist. Ist nämlich p eine Primzahl, die in M aufgeht, und geht erstens p nicht in a_0 auf, so setze man

$$t \equiv 0 \mod. p.$$

Geht zweitens p in a_0 auf, dann setze man

$$t \not\equiv 0 \mod. p$$

$$t \not\equiv -\frac{2\alpha_0}{A_1} \mod. p.$$

Die zweite Bedingung ist sinnvoll, da p als Teiler von M nicht in A_1 aufgeht. Sie ist mit der ersten vereinbar, auch für $p = 2$, wo sie mit ihr zusammenfällt. Beide Bedingungen ergeben:

$$2t\alpha_0 + t^2 A_1 = t(2\alpha_0 + tA_1) \not\equiv 0 \mod. p$$

Immer wird dann

$$a \not\equiv 0 \mod. p,$$

VI, 42 also zusammengenommen a prim zu M. Also ist

$$\begin{array}{lcl} x_1 & \rightarrow & \frac{\alpha}{a} x_1 + \left(\frac{\alpha}{a} - 1\right) x_2 \\ x_2 & \rightarrow & x_1 + x_2 \end{array}$$

eine für M ganze unimodulare Transformation. Durch sie geht in der Tat φ über in die ganzzahlige binäre Form

$$\Phi = A_1 x_1^2 + 2(A_1 - \alpha)x_1 x_2 + (A_1 - 2\alpha + a)x_2^2$$

der Ordnung $\left(\begin{array}{c|c} o_1 & 0 \\ 1 & \end{array}\right)$ mit den Hauptunterdeterminanten

$$A_0 = 1\,, \quad A_1\,, \quad A_2 o_1 = o_1\,,$$

also eine charakteristische Form für M, aus der φ in der genannten Weise entsteht.

Diese Betrachtungen seien jetzt angewandt auf die binäre Form

$$\varphi = A_1 x_1^2 + \frac{1}{A_1} A_2 o_1 x_2^2,$$

die aus f durch $x_3 = 0, \ldots, x_n = 0$ hervorgeht. Nach der ersten Bedingung (1) ist für sie das Analogon zu (1') erfüllt. Also ist φ Normalgestalt einer charakteristischen Form Φ für M, die zur Ordnung $\left(\begin{matrix} A_2 o_1 \\ 1 \end{matrix} \middle| \, 0 \right)$ gehört. VI, 43

Es werde nun eine zu M prime Primzahl p mit den Eigenschaften

$$\left\{ \frac{p}{A_2 o_1} \right\} = \left\{ \frac{A_1}{A_2 o_1} \right\} \tag{2}$$

bestimmt, d. h. also, es soll p dieselben Geschlechtscharaktere besitzen, wie der erste Koeffizient A_1 von Φ, bezogen auf die Ordnung $\left(\begin{matrix} A_2 o_1 \\ 1 \end{matrix} \middle| \, 0 \right)$. Ich betrachte dann die binäre Form

$$\overline{\varphi} = p x_1^2 + \frac{1}{p} A_2 o_1 x_2^2.$$

Die Bedingung dafür, daß auch sie Normalgestalt einer charakteristischen Form der betrachteten Ordnung ist, lautet

$$\left(\frac{-A_2 o_1}{p} \right) = 1. \tag{3}$$

Um diese Bedingung zu erfüllen, werde für $n \geqq 4$ noch

$$p \equiv 1 \bmod. 4 \tag{4}$$

vorgeschrieben. Dann ist in der Tat: VI, 44

$$\left(\frac{-A_2 o_1}{p} \right) = \left(\frac{p}{-A_2 o_1} \right) = \left(\frac{A_1}{-A_2 o_1} \right) = \left(\frac{-A_2 o_1}{A_1} \right) = 1$$

wegen $A_1 \equiv 1 \bmod. 4$ und nach (1), (2).

Für $n = 3$ hat man nach (1), (2):

$$\begin{aligned}
\left(\frac{-A_2 o_1}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{-A_2 o_1 - 1}{2}} \left(\frac{p}{-A_2 o_1}\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{-A_2 o_1 - 1}{2}} \cdot \left(\frac{A_1}{-A_2 o_1}\right) \\
&= (-1)^{\frac{p-1}{2}\cdot\frac{-A_2 o_1 - 1}{2} + \frac{A_1 - 1}{2}\cdot\frac{-A_2 o_1 - 1}{2}} \cdot \left(\frac{-A_2 o_1}{A_1}\right) \\
\left(\frac{-A_2 o_1}{p}\right) &= (-1)^{\frac{pA_1-1}{2}\cdot\frac{-A_2 o_1 - 1}{2}}
\end{aligned}$$

Wird also hier statt (4) vorgeschrieben:

(4') $\quad p \equiv A_1 \mod 4$, falls $-A_2 o_1 \equiv -1 \mod 4$,

so ist wiederum (3) erfüllt. Ich zeige, daß diese zunächst von A_1, A_2 abhängige Vorschrift *nur* vom Geschlecht der Ausgangsform abhängt, also von den Charakteren

VI, 45

$$\left\{\frac{A_1}{o_1}\right\}, \quad \left\{\frac{A_2}{o_2}\right\}.$$

In der Tat folgt aus (1):

$$\left(\frac{-A_2 o_1}{-A_1 o_2}\right) \cdot \left(\frac{-A_1 o_2}{-A_2 o_1}\right) = (-1)^{1+\frac{-A_2 o_1 - 1}{2}\cdot\frac{-A_1 o_2 - 1}{2}}$$
$$= \left(\frac{-A_2 o_1}{o_2}\right) \cdot \left(\frac{-A_1 o_2}{o_1}\right) = \text{Geschlechtsinvariante},$$

also die Invarianz von

$$\frac{-A_2 o_1 - 1}{2} \cdot \frac{-A_1 o_2 - 1}{2} \mod 2.$$

Hiernach ist sowohl die Kongruenz $\frac{-A_2 o_1 - 1}{2} \equiv 1 \mod 2$, als auch — wenn sie erfüllt ist — der Wert $A_1 \mod 4$ geschlechtsinvariant. Damit ist in allen Fällen (3) durch eine geschlechtsinvariante Vorschrift für p gesichert.

VI, 46

Ich setze nunmehr die Behauptung für $n = 2$ als bewiesen voraus — sie folgt da in bekannter Weise aus der klassischen Theorie der binären quadratischen Formen —, und verwende dann vollständige Induktion. Die Induktionsannahme soll sogar folgendermaßen lauten: Zwei „Normalgestalten“, für die Ordnung und

Geschlechtscharaktere übereinstimmen und die Bedingungen (1) erfüllt sind, außerdem bei mehr als ternären Formen die ersten $n-3$ Koeffizienten $\equiv 1 \mod 4$ sind, sind durch unimodulare für M ganze Transformation auseinander herleitbar, ungeachtet ob sie aus charakteristischen Formen entspringen, oder nicht. Für $n=2$ ist das nach dem Bewiesenen nicht allgemeiner, also nach der Voraussetzung richtig. Für $n>2$ füge ich noch die Einschränkung hinzu, daß die Koeffizienten A_i, B_i zueinander prim sein sollen, was stets (durch passende Wahl des M bei der zweiten Form) erreichbar ist. Die zweite Normalgestalt sei: VI, 47

$$g = B_1 x_1^2 + \frac{B_2}{B_1} o_1 x_2^2 + \cdots + \frac{B_{n-1}}{B_{n-2}} o_1 \cdots o_{n-2} x_{n-1}^2 + \frac{1}{B_n} o_1 \cdots o_{n-1} x_n^2$$

Die Geschlechtscharaktere stimmen mit denen von f überein:

$$\left\{\frac{A_\nu}{o_\nu}\right\} = \left\{\frac{B_\nu}{o_\nu}\right\}, \quad (\nu = 1, \ldots, n-1) \tag{5}$$

Da zudem A_2, B_2 zueinander prim sein sollen, so kann p zu f und g gemeinsam, den Forderungen (2) entsprechend bestimmt werden. Da auch die übrigen Forderungen (4), (4') geschlechtsinvariant sind $\big((4)$ nach Konstruktion$\big)$, so kann also die Bestimmung von p überhaupt vollständig für f und g gemeinsam durchgeführt werden.

Nach dieser Konstruktion ist nun φ mit $\overline{\varphi}$ im gleichen Geschlecht, also nach Voraussetzung für M ganzzahlig äquivalent, also auch f mit VI, 48

$$\overline{f} = p x_1^2 + \frac{o_1}{p}\left[A_2 x_2^2 + \frac{A_3}{A_2}(p o_2) x_3^2 + \cdots + \frac{1}{A_{n-1}}(p o_2) \cdots o_{n-1} x_n^2\right],$$

ebenso auch g mit

$$\overline{g} = p x_1^2 + \frac{o_1}{p}\left[B_2 x_2^2 + \frac{B_3}{B_2}(p o_2) x_3^2 + \cdots + \frac{1}{B_{n-1}}(p o_2) \cdots o_{n-1} x_n^2\right].$$

Es werde

$$\overline{f} = p x_1^2 + \frac{o_1}{p} f_0$$
$$\overline{g} = p x_1^2 + \frac{o_1}{p} g_0$$

gesetzt. Dann sind f_0 und g_0 Normalgestalten der Ordnung

$$\left(\begin{array}{cccc|c} p o_2, & o_3, & \ldots, & o_{n-1} & \multirow{2}{*}{0} \\ 1, & 1, & \ldots, & 1 & \end{array}\right).$$

In der Tat sind nach (1) alle Bedingungen dazu erfüllt bis auf ev.

$$\left\{\frac{-A_3 p o_2}{A_2}\right\} = 1.$$

Das folgt aber aus (1) nach (2). Ferner gehören f_0, g_0 zum gleichen Geschlecht. Denn nach (5) sind alle Bedingungen dazu erfüllt, bis auf ev.

$$\left(\frac{A_2}{p}\right) = \left(\frac{B_2}{p}\right).$$

VI, 49 Das folgt aber aus (3). Schließlich genügen f_0, g_0 nach Konstruktion auch den Zusatzvoraussetzungen der Induktionsannahme. Also sind, nach dieser, f_0 und g_0 für M ganzz. äquivalent. Damit sind es auch $\overline{f}$ und $\overline{g}$, sowie f und g, w. z. b. w.

6.9 Normentheorie in Ringen. (Feb.1929)

These are Hasse's notes of a colloquium talk of Heinrich Grell (a Ph.D. student of Emmy Noether). The topic is the definition of norms in a finite extension of a Dedekind ring. Grell had published this 1927 in the "Mathematische Annalen" [Gre27].

VI, 50

(Nach Vortrag von H. Grell, Februar 1929).

I.) Es seien zunächst vorgegeben:

$\mathfrak{o}$, ein Ring, in dem die ersten vier der E. Noetherschen Axiome gelten

$\mathfrak{z}$, ein darin enthaltener Ring, in dem die fünf E. Noetherschen Axiome gelten und zudem jedes Ideal Hauptideal ist. Es soll $\mathfrak{o}$ ein $\mathfrak{z}$–Modul von endlichem Range n sein.

Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$ und

$$\alpha_i = \sum_{k=1}^{n} a_{ik}\omega_k \qquad (i = 1, \ldots, n)$$

die Darstellung einer $\mathfrak{z}$–Modulbasis von $\mathfrak{a}$ durch eine solche von $\mathfrak{o}$, so werde definiert

$$N(\mathfrak{a}) = |a_{ik}|\mathfrak{z},$$

also gleich dem aus der Determinante $|a_{ik}|$ abgeleiteten Hauptideal in $\mathfrak{z}$. Das ist von der speziellen Auswahl der Basen unabhängig. Allgemein werde bezeichnet mit $(\mathfrak{ab}, \mathfrak{b})$ das aus der Übergangsdeterminante von einer Basis von $\mathfrak{b}$ zu einer von $\mathfrak{ab}$ abgeleitete Hauptideal in $\mathfrak{z}$, das wieder von der speziellen Wahl der Basen unabhängig ist. Also $N(\mathfrak{a}) = (\mathfrak{a}, \mathfrak{o})$. VI, 51

Satz 1. *Ist* $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$ *die Primärzerlegung eines Ideals* $\mathfrak{a}$ *aus* $\mathfrak{o}$*, so gilt*

$$N(\mathfrak{a}) = N(\mathfrak{q}_1) \cdots N(\mathfrak{q}_s).$$

Beweis: Es ist

$$N(\mathfrak{a}) = (\mathfrak{a}, \mathfrak{o}) = (\mathfrak{q}_1 \cdots \mathfrak{q}_s, \mathfrak{q}_1 \cdots \mathfrak{q}_{s-1}) \cdots (\mathfrak{q}_1\mathfrak{q}_2, \mathfrak{q}_1)(\mathfrak{q}_1, \mathfrak{o}).$$

Zum Beweis genügt es, zu zeigen, daß immer

$$(\mathfrak{ab}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{o})$$

ist, wenn $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind:

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{o}$$

ist. Nun gilt die Isomorphie

$$\mathfrak{a} + \mathfrak{b}|\mathfrak{a} \overset{+}{\underset{\cdot}{\longleftrightarrow}} \mathfrak{b}|\mathfrak{a} \cap \mathfrak{b}$$

für beliebige $\mathfrak{a}$ und $\mathfrak{b}$, wenn allgemein $\mathfrak{c}/\mathfrak{d}$ den Restklassenring von $\mathfrak{c}$ nach dem Vielfachen $\mathfrak{d}$ bezeichnet und $\mathfrak{a} \cap \mathfrak{b}$ den Durchschnitt (kl. gem. Vielfache). Es ist das der zweite E. Noethersche Isomorphiesatz (Verallgemeinerung meines

VI, 52

Reduktionsprinzips).Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd, so ist in $\mathfrak{o}$ nach der Voraussetzung $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$, also gilt dann

$$\mathfrak{o}|\mathfrak{a} \overset{+}{\underset{\cdot}{\longleftrightarrow}} \mathfrak{b}|\mathfrak{ab}.$$

Nun ist allgemein $\mathfrak{b}/\mathfrak{ab}$ eine verallgemeinerte Abelsche Gruppe bezüglich der Addition mit $\mathfrak{z}$ als Multiplikatorenbereich. Ist $\beta_1, \ldots, \beta_n$ eine $\mathfrak{z}$–Modulbasis von $\mathfrak{b}$ und $\gamma_1, \ldots, \gamma_n$ eine solche von $\mathfrak{ab}$, ferner

$$\gamma_i = \sum_{k=1}^{n} c_{ik}\beta_k\,, \qquad (i = 1, \ldots, n)$$

so sind die Relationen

$$\gamma_i = \sum_{k=1}^{n} c_{ik}\beta_k \equiv 0 \ (\mathfrak{ab})$$

erzeugende Relationen jener v. Ab. Gruppe. Nach der Voraussetzung über $\mathfrak{z}$ lassen sich diese Relationen in der bei den gew. Ab. Gruppen bekannten Weise auf die Normalform

$$\gamma_i' = e_i\beta_i' \equiv 0 \ (\mathfrak{ab})$$

transformieren. Die e_i sind die Elementarteiler der Matrix (c_{ik}). Sie (besser: die aus ihnen abgel. Hauptid. $e_i\mathfrak{z}$) sind charakteristisch für die Struktur der v. Ab. Gruppe, ebenso wie bei den gew. Ab. Gruppen. Die beiden isomorphen

VI, 53

v. Ab. Gruppen $\mathfrak{o}|\mathfrak{a}$ und $\mathfrak{b}|\mathfrak{ab}$ haben also gleiche Elementarteiler. Das Produkt

der Elementarteiler ist nun aber die Determinante der Übergangssubstitution zwischen den betr. Basen. Also folgt in der Tat

$$(\mathfrak{a}\mathfrak{b}, \mathfrak{b}) = (\mathfrak{a}, \mathfrak{o}), \qquad \text{w. z. b. w.}$$

Satz 2. *Ist* $\mathfrak{q}$ *ein Primärideal aus* $\mathfrak{o}$*, ferner* $\mathfrak{p}$ *das zugehörige Primideal und* λ *die Länge der Kompositionsreihen (aus Idealteilern) der v. Ab. Gruppe* $\mathfrak{o}|\mathfrak{q}$*, so gilt*

$$N(\mathfrak{q}) = N(\mathfrak{p})^\lambda$$

Beweis: Zunächst gilt für die Kompositionsreihen aus Idealteilern das Analogon zum Jordan–Hölderschen Satz, wie man leicht mittels des zweiten Isomorphiesatzes von E. Noether (siehe oben) beweist. Also ist die Länge λ durch $\mathfrak{q}$ eindeutig bestimmt. Sei nun

$$\mathfrak{o} = \mathfrak{q}_0, \mathfrak{p} = \mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q} = \mathfrak{q}_\lambda$$

eine Kompositionsreihe von $\mathfrak{q}$. Dann ist

$$N(\mathfrak{q}) = (\mathfrak{q}, \mathfrak{o}) = (\mathfrak{q}_\lambda, \mathfrak{q}_{\lambda-1}), \ldots (\mathfrak{q}_1, \mathfrak{q}_0).$$

Nach den Schlüssen aus dem Beweise von Satz 1 genügt es, die Isomorphie VI, 54

$$\mathfrak{q}_i|\mathfrak{q}_{i+1} \overset{+}{\underset{\cdot}{\longleftrightarrow}} \mathfrak{o}|\mathfrak{p}$$

zu beweisen.

Dazu muß zunächst der folgende Hilfssatz bewiesen werden:

Hilfssatz: *Ist* $\mathfrak{q}$ *primär* $\mathfrak{p}$ *das zugehörige Primideal und* $\mathfrak{a}$ *ein unmittelbarer echter Teiler von* $\mathfrak{q}$ *(d. h. zwischen* $\mathfrak{a}$ *und* $\mathfrak{q}$ *kein Ideal mehr), so ist* $\mathfrak{q} : \mathfrak{p}$ *Teiler von* $\mathfrak{a}$*, also*

$$\mathfrak{q} : \mathfrak{p}|\mathfrak{a}|\mathfrak{q}.$$

Beweis: Bekanntlich existiert ein ϱ, sodaß $\mathfrak{q}|\mathfrak{p}^\varrho$, also $\mathfrak{q} : \mathfrak{p}^\varrho = \mathfrak{o}$. Wegen $\mathfrak{q} : \mathfrak{p}^\varrho = \mathfrak{o}|\mathfrak{a}$ aber $\mathfrak{q} : \mathfrak{p}^0 = \mathfrak{q} \nmid \mathfrak{a}$ gibt es einen echten positiven Exponenten σ, sodaß

$$\text{noch} \quad \mathfrak{q} : \mathfrak{p}^{\sigma-1} \nmid \mathfrak{a}, \qquad \text{aber} \quad \mathfrak{q} : \mathfrak{p}^\sigma|\mathfrak{a}.$$

D. h.

$$\text{noch} \quad \mathfrak{q} \nmid \mathfrak{p}^{\sigma-1}\mathfrak{a}, \qquad \text{aber} \quad \mathfrak{q}|\mathfrak{p}^\sigma\mathfrak{a}.$$

Aus $\mathfrak{a}|\mathfrak{q}$ und $\mathfrak{a}|\mathfrak{p}^{\sigma-1}\mathfrak{a}$ folgt nun

$$\mathfrak{a}|\mathfrak{q} + \mathfrak{p}^{\sigma-1}\mathfrak{a}, \tag{1}$$

VI, 55 andererseits ist

$$(2) \qquad \mathfrak{q} + \mathfrak{p}^{\sigma-1}\mathfrak{a} | \mathfrak{q} \quad \text{und zwar echt,}$$

weil aus $\mathfrak{q} + \mathfrak{p}^{\sigma-1}\mathfrak{a} = \mathfrak{q}$ folgte $\mathfrak{q}|\mathfrak{p}^{\sigma-1}\mathfrak{a}$. Nach der Voraussetzung ergibt sich aus (1) und (2):

$$\mathfrak{q} + \mathfrak{p}^{\sigma-1}\mathfrak{a} = \mathfrak{a},$$

also

$$\mathfrak{p}\mathfrak{q} + \mathfrak{p}^{\sigma}\mathfrak{a} = \mathfrak{p}\mathfrak{a}.$$

Wegen $\mathfrak{q}|\mathfrak{p}^{\sigma}\mathfrak{a}$ ist daher

$$\mathfrak{q}|\mathfrak{p}\mathfrak{a}, \quad \text{d. h.} \quad \mathfrak{q} : \mathfrak{p}|\mathfrak{a}, \qquad \text{w. z. b. w.}$$

Fortsetzung des Beweises von Satz 2. Es sei π_i eine Zahl aus $\mathfrak{o}$ mit den Eigenschaften

$$\pi_i \equiv 0 \ (\mathfrak{q}_i), \quad \not\equiv 0 \ (\mathfrak{q}_{i+1}).$$

Um die obige Isomorphie zu beweisen, genügt es, nach dem zweiten E. Noetherschen Isomorphiesatz, die beiden Feststellungen

$$1.) \qquad \pi_i\mathfrak{o} + \mathfrak{q}_{i+1} = \mathfrak{q}_i$$
$$2.) \qquad \pi_i\mathfrak{o} \cap \mathfrak{q}_{i+1} = \pi_i\mathfrak{p}$$

zu machen; denn daraus folgt

$$\mathfrak{q}_i|\mathfrak{q}_{i+1} \overset{+}{\underset{\cdot}{\longleftrightarrow}} \pi_i\mathfrak{o} + \mathfrak{q}_{i+1}|\mathfrak{q}_{i+1} \quad \overset{+}{\underset{\cdot}{\longleftrightarrow}} \quad \pi_i\mathfrak{o}|\pi_i\mathfrak{o} \cap \mathfrak{q}_{i+1}$$
$$\overset{+}{\underset{\cdot}{\longleftrightarrow}} \quad \pi_i\mathfrak{o}|\pi_i\mathfrak{p} \overset{+}{\underset{\cdot}{\longleftrightarrow}} \mathfrak{o}|\mathfrak{p}.$$

VI, 56 ad 1.) $\pi_i\mathfrak{o} + \mathfrak{q}_{i+1}$ ist ein Ideal zwischen $\mathfrak{q}_i$ und $\mathfrak{q}_{i+1}$, und von $\mathfrak{q}_{i+1}$ verschieden, nach Wahl von π_i, also gleich $\mathfrak{q}_i$ wegen der Eigenschaft der Kompositionsreihe, aus lauter unmittelbaren echten Teilern aufgebaut zu sein.

ad 2.) $\pi_i\mathfrak{p}$ ist Vielfaches von $\pi_i\mathfrak{o}$ und $\mathfrak{q}_{i+1}$, letzteres nach dem Hilfssatz, der ergibt, daß $\mathfrak{q}_{i+1} : \mathfrak{p}$ Teiler von $\mathfrak{q}_i$, also von π_i, also $\mathfrak{q}_{i+1}$ Teiler von $\pi_i\mathfrak{p}$ ist. Umgekehrt sei δ eine Zahl aus $\pi_i\mathfrak{o}$ und $\mathfrak{q}_{i+1}$. Sie hat die Form $\delta = \pi_i\gamma$ mit ganzem γ, und es ist

$$\pi_i\gamma \equiv 0 \ (\mathfrak{q}_{i+1}).$$

Wäre

$$\gamma \not\equiv 0 \ (\mathfrak{p}),$$

so wäre γ kein Nullteiler mod. $\mathfrak{q}_{i+1}$, also folgte

$$\pi_i \equiv 0 \ (\mathfrak{q}_{i+1}),$$

was falsch. Also folgt

$$\gamma \equiv 0 \ (\mathfrak{p}),$$

und somit

$$\delta \equiv 0 \ (\pi_i \mathfrak{p}).$$

Damit ist der Beweis von Satz 2 erbracht. **Satz 3.** *Ist außer* $\mathfrak{z}$ *und* $\mathfrak{o}$ *noch ein Ring* $\mathfrak{r}$ *zwischen* $\mathfrak{z}$ *und* $\mathfrak{o}$ *gegeben, über den die gleichen Voraussetzungen gelten, wie über* $\mathfrak{z}$*, so gilt für* $\mathfrak{a}$ *aus* $\mathfrak{o}$: VI, 57

$$N_{\mathfrak{z}}(\mathfrak{a}) = N_{\mathfrak{z}}\big(N_{\mathfrak{r}}(\mathfrak{a})\big),$$

wo der an das Normzeichen gesetzte Ring den Grundring angibt, in bezug auf den die Norm zu nehmen ist.

Beweis: Es seien

$$\begin{aligned} \mathfrak{a} &= (\alpha_1, \dots, \alpha_n)_{\mathfrak{r}} \\ \mathfrak{o} &= (\omega_1, \dots, \omega_m)_{\mathfrak{r}} \qquad (mr = n) \\ \mathfrak{r} &= (\varrho_1, \dots, \varrho_r)_{\mathfrak{z}} \end{aligned}$$

Modulbasen in bezug auf die angegebenen Ringe. Durch Transformation auf die Normalform darf ohne Einschränkung angenommen werden, daß die Übergangs-substitution von $\mathfrak{o}$ nach $\mathfrak{a}$ in bezug auf $\mathfrak{r}$ so beschaffen ist:

$$\alpha_i = e_i \omega_i \qquad (i = 1, \dots, m)$$

mit e_i aus $\mathfrak{r}$. Nun ist

$$\begin{aligned} \mathfrak{a} &= (\alpha_i \varrho_k)_{\mathfrak{z}} \\ \mathfrak{o} &= (\omega_i \varrho_k)_{\mathfrak{z}} \,. \end{aligned}$$

VI, 58 Die Übergangssubstitution von $\mathfrak{o}$ nach $\mathfrak{a}$ in bezug auf $\mathfrak{z}$ findet sich dann so:

$$e_i \varrho_k = \sum_{\ell=1}^{r} a_{ik\ell} \varrho_\ell \qquad \begin{pmatrix} i = 1, \dots, m \\ k = 1, \dots, r \end{pmatrix}$$

$$\alpha_i \varrho_k = e_i \varrho_k \omega_i = \sum_{\ell=1}^{r} a_{ik\ell} \omega_i \varrho_\ell$$

Die Übergangsmatrix sieht, wenn man zuerst nach i und bei festem i nach k bzw. ℓ ordnet, so aus

$$\begin{pmatrix} (a_{1k\ell}) & 0 & \cdots & 0 \\ 0 & (a_{ik\ell}) & \cdots & 0 \\ \multicolumn{4}{c}{\dots\dots\dots\dots\dots\dots\dots} \\ 0 & \multicolumn{2}{c}{\dots\dots\dots} & (a_{mk\ell}) \end{pmatrix},$$

entsteht also aus der ursprünglichen $\begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_r \end{pmatrix}$, indem e_i durch die Matrix $(a_{ik\ell})$ ersetzt wird. Hieraus folgt:

$$N_{\mathfrak{z}}(\mathfrak{a}) = |a_{1k\ell}| \cdots |a_{mk\ell}| \mathfrak{z}.$$

Nun ist

$$N_{\mathfrak{z}}(e_i \mathfrak{r}) = |a_{ik\ell}| \mathfrak{z}\,, \qquad N_{\mathfrak{r}}(\mathfrak{a}) = e_1 \cdots e_m \mathfrak{r}$$

also

$$\begin{aligned} N_{\mathfrak{z}}(\mathfrak{a}) &= N_{\mathfrak{z}}(e_1 \mathfrak{r}) \cdots N_{\mathfrak{z}}(e_m \mathfrak{r}) \\ &= N_{\mathfrak{z}}(e_1 \cdots e_m \mathfrak{r}) = N_{\mathfrak{z}}\big(N_r(\mathfrak{a})\big). \end{aligned}$$

VI, 59 Dabei ist zu bedenken, daß im Ring $\mathfrak{r}$ nach Satz 1 und Satz 2 die Formel $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ allgemein gilt.

II.) Es soll jetzt gezeigt werden, daß in den Sätzen 1—3 die Voraussetzungen über $\mathfrak{z}$ und $\mathfrak{r}$ gelockert werden können. Es braucht nämlich nur vorausgesetzt zu werden, daß in $\mathfrak{z}$ und $\mathfrak{r}$ die fünf E. Noetherschen Axiome gelten, nicht daß jedes Ideal Hauptideal ist.

Es genügt, die Definition von $N(\mathfrak{a})$ zu verallgemeinern; die Durchführung der Beweise gelingt dann ohne Schwierigkeiten.

Sei dazu $m\mathfrak{z}$ ein beliebiges Vielfaches von $\mathfrak{a}\mathfrak{z}$. Dann sei $\mathfrak{z}'$ der Ring aller Quotienten mit zu m primem Nenner aus Zahlen von $\mathfrak{z}$ und ebenso $\mathfrak{o}'$ der Ring aller Quotienten mit zu $m\mathfrak{r}$ primem Nenner aus Zahlen von $\mathfrak{o}$. Dann sind bekanntlich in $\mathfrak{z}'$ alle Ideale Hauptideale. Ferner ist

$$\mathfrak{o}' = (\omega_1, \ldots, \omega_n)_{\mathfrak{z}}\,, \quad \text{wenn} \quad \mathfrak{o} = (\omega_1, \ldots, \omega_n)_{\mathfrak{z}}$$
$$\mathfrak{a}' = (\alpha_1, \ldots, \alpha_n)_{\mathfrak{z}'}\,, \quad \text{"} \quad \mathfrak{a} = (\alpha_1, \ldots, \alpha_n)_{\mathfrak{z}}$$

ist, d. h. die alten Modulbasen können übernommen werden. Schließlich entsprechen sich hinsichtlich aller Idealoperationen isomorph die Teiler von $\mathfrak{a}$ in $\mathfrak{o}$ und die von $\mathfrak{a}\mathfrak{o}'$ in $\mathfrak{o}'$, sogar die von $m\mathfrak{o}$ in $\mathfrak{o}$ und die von $m\mathfrak{o}'$ in $\mathfrak{o}'$, ebenso die von $m\mathfrak{z}$ in $\mathfrak{z}$ und $m\mathfrak{z}'$ in $\mathfrak{z}'$. Jetzt werde definiert: VI, 60

$$N_{\mathfrak{z}}(\mathfrak{a}) = N_{\mathfrak{z}'}(\mathfrak{a}\mathfrak{o}') \cap \mathfrak{z}.$$

Diese Definition erweist sich als unabhängig von der Hilfszahl m, eben weil die Basen übernommen werden können.

Auf diese Weise wird der allgemeine Fall II.) auf den speziellen Fall I.) zurückgeführt.

III.) Es bleibt noch die Identität der Normdefinition mit der üblichen (Produkt der konjugierten) nachzuweisen. Voraussetzung dabei ist aber, daß auch in $\mathfrak{o}$ die fünf E. Noetherschen Axiome gelten. Ferner, daß der Quotientenkörper zu $\mathfrak{o}$ relativ–Galoissch 1. Art über dem zu $\mathfrak{z}$ ist. (Im allgemeinen läßt sich $\mathfrak{o}$ in einen solchen Galoisschen Erweiterungsring einbetten). Dann gilt

$$N(\mathfrak{a}) = \mathfrak{a}\mathfrak{a}^{(1)} \cdots \mathfrak{a}^{(n-1)},$$

wenn obere Indizes die in Bezug auf $\mathfrak{z}$ konjugierten bezeichnen. Durch das Verfahren von II.) führt man die Behauptung auf den Fall zurück, daß $\mathfrak{z}$ und jetzt auch $\mathfrak{o}$ Hauptidealringe sind. Dann sei VI, 61

$$\mathfrak{a} = \alpha\mathfrak{o}$$

Es ist dann

$$\mathfrak{a} = (\alpha\omega_1, \ldots, \alpha\omega_n)_{\mathfrak{z}}\,, \quad \text{wenn} \quad \mathfrak{o} = (\omega_1, \ldots, \omega_n)_{\mathfrak{z}}$$

ist. Aus

$$\alpha\omega_i = \sum_{k=1}^{n} a_{ik}\omega_k \qquad (i = 1, \ldots, n)$$

folgt nun durch Übergang zu den relativ–konjugierten:

$$\alpha^{(\nu)}\omega_i^{(\nu)} = \sum_{k=1}^{n} a_{ik}\omega_k^{(\nu)}$$

und daraus:

$$\alpha^{(1)} \cdots \alpha^{(n)} |\omega_i^{(k)}| = |a_{ik}| \cdot |\omega_i^{(k)}|$$

Da $\mathfrak{o}$ von der 1. Art, ist $|\omega_i^{(k)}| \neq 0$, also

$$N(\mathfrak{a}) = |a_{ik}|\mathfrak{z} = \alpha^{(1)} \cdots \alpha^{(n)}\mathfrak{z} = \mathfrak{a}^{(1)} \cdots \mathfrak{a}^{(n)}.$$

6.10 Über eine Frage von Z.Suetuna. (29.7.1929)

The question concerns permutation groups. Suetuna had sooved the question for certain special groups and Hasse now provides a general proof, valid for arbitrary permutation groups. The Japanese mathematician Suetuna was visiting Göttingen and Hamburg in the years 1927-1931. He also had a joint paper with Hasse [HS31]. *1936 Suetuna became the successor of Takagi at Tokyo University.*

VI, 62

29. 7. 29.

Suetuna vermutet folgendes: Gegeben eine endliche Permutationsgruppe $\mathfrak{G}$ vom Grade n und der Ordnung g. Mit $e(\mathsf{S})$ sei die Anzahl der Zyklen bezeichnet, in die das Gruppenelement S zerfällt. Dann ist die Summe

$$A(a) = \frac{1}{g} \sum_{\mathsf{S} \text{ in } \mathfrak{G}} a^{e(\mathsf{S})} \tag{1}$$

für jedes ganze a ganz. Noch allgemeiner gilt dasselbe für jede Summe

$$A_i(a) = \frac{1}{g} \sum_{\mathsf{S} \text{ in } \mathfrak{G}} \chi_i(\mathsf{S}) a^{e(\mathsf{S})}, \tag{2}$$

wo $\chi_i(\mathsf{S})$ irgendeinen Frobeniusschen Gruppencharakter von $\mathfrak{G}$ durchläuft.

Suetuna beweist die spezielle Vermutung (1) für zwei Fälle, erstens für die allgemeine lineare Gruppe von Primzahlpotenzgrad: VI, 63

$$\begin{pmatrix} \nu \\ r\nu + s \end{pmatrix} \quad \bigl(s = 0, \dots, p^k - 1;\ (r,p) = 1\bigr),$$

zweitens für den Fall $g = n$, der der Galoisschen Gruppe eines Galoisschen Zahlkörpers n–ten Grades entspricht.

1.) Ich füge nachstehend den Beweis von (1) für den Fall $g = n!$ hinzu, der der Galoisschen Gruppe eines affektlosen Zahlkörpers n–ten Grades entspricht. $\mathfrak{G}$ ist dann die symmetrische Gruppe n–ten Grades.

Ist nun S eine Permutation mit ν_i Zyklen i–ten Grades ($i = 1, \dots, n$), so bleibt S bei genau $\nu_1! 1^{\nu_1} \cdot \nu_2! 2^{\nu_2} \dots \cdot \nu_n! n^{\nu_n}$ Permutationen der Ziffern in den Zyklen invariant; denn es können ja die ν_i i–gliedrigen Zyklen auf $\nu_i!$ Arten angeordnet und dann die Ziffern in jedem einzelnen noch auf i Arten gesetzt

werden. Folglich entstehen aus S insgesamt $\frac{n!}{\nu_1!1^{\nu_1}\cdots\nu_n!n^{\nu_n}}$ Permutationen des
VI, 64 gleichen Typus $(\nu_1,\ldots,\nu_n)$ der Zyklenzerlegung. Daher ist die zu untersuchende Summe:

$$A_n(a) = \sum_{\substack{\nu_1+2\nu_2+\cdots+n\nu_n=n \\ \nu_i\geqq 0}} \frac{a^{\nu_1+\nu_2+\cdots+\nu_n}}{\nu_1!1^{\nu_1}\cdot\nu_2!2^{\nu_2}\cdots\nu_n!n^{\nu_n}}\,.$$

Hierin können ohne Änderung statt der endlichen Folge $\nu_1,\ldots,\nu_n$ von Summationsbuchstaben deren unendlich viele $\nu_1,\nu_2,\ldots$ mit der Nebenbedingung $\nu_1+2\nu_2+\cdots=n$ eingeführt werden:

$$A_n(a) = \sum_{\substack{\nu_1+2\nu_2+\cdots=n \\ \nu_i\geqq 0}} \frac{1}{\nu_1!}\left(\frac{a}{1}\right)^{\nu_1}\cdot\frac{1}{\nu_2!}\left(\frac{a}{2}\right)^{\nu_2}\cdot\cdots.$$

Jetzt bilde ich die erzeugende Funktion der $A_n(a)$ und finde:

$$\begin{aligned}
\sum_{n=0}^{\infty} A_n(a)x^n &= \sum_{\nu_i\geqq 0}\frac{1}{\nu_1!}\left(\frac{a}{1}\right)^{\nu_1}x^{\nu_1}\cdot\frac{1}{\nu_2!}\left(\frac{a}{2}\right)^{\nu_2}x^{2\nu_2}\cdots \\
&= \sum_{\nu_i\geqq 0}\frac{1}{\nu_1!}\left(\frac{ax}{1}\right)^{\nu_1}\frac{1}{\nu_2!}\left(\frac{ax^2}{2}\right)^{\nu_2}\cdots \\
&= e^{\frac{ax}{1}}\cdot e^{\frac{ax^2}{2}}\cdots \\
&= e^{a\left(\frac{x}{1}+\frac{x^2}{2}+\cdots\right)} \\
&= e^{a\lg\frac{1}{1-x}} = e^{\lg\frac{1}{(1-x)^a}} = \frac{1}{(1-x)^a}\,.
\end{aligned}$$

VI, 65 Also

$$\sum_{n=0}^{\infty} A_n(a)x^n = \sum_{n=0}^{\infty}\binom{a+n-1}{n}x^n$$

$$A_n(a) = \binom{a+n-1}{n},$$

woraus die Ganzzahligkeit folgt.

2.) Die allgemeine Formel (2) läßt sich für die symmetrische Gruppe n–ten Grades $\mathfrak{G}$ aus den Resultaten der I. Schurschen Dissertation folgern. (Berlin 1901).

Es sei $m \geqq n$ fest. Die nicht singulären Darstellungen Γ von $\mathfrak{G}$ stehen dann nach I. Schur, l. c. in eineindeutiger Korrespondenz mit den Darstellungen M der reellen Matrixalgebra m–ten Grades $\mathfrak{M}$ aus einem Körper der Charakteristik 0 durch nicht durchweg singuläre Matrizen, die homogen von der Dimension n sind*) in den Elementen der Matrizen aus $\mathfrak{M}$. Äquivalenten Γ entsprechen äquivalente M und umgekehrt, reduziblen Γ reduzible M und umgekehrt.

Um Γ von M aus zu erhalten, denke man zunächst M unter äquivalenten so ausgewählt, daß Diagonalmatrizen aus $\mathfrak{M}$ Diagonalmatrizen in M entsprechen, was nach Schur, l. c. stets möglich ist. Nunmehr sei P eine Permutation aus $\mathfrak{G}$. VI, 66 Diese kann als Permutationsmatrix n–ten Grades gedacht und zu einer Matrix m–ten Grades durch Nullreihen aufgefüllt werden. Dann entspricht diesem Element P aus $\mathfrak{M}$ ein bestimmtes Element $\varphi(\mathsf{P})$ aus M. Wegen der Homogenität ist $\varphi(\mathsf{P})$ nur in einem ganz bestimmten, zur Hauptdiagonale symmetrischen Feld besetzt und hat dort von 0 verschiedene Determinante. Diese verkürzten $\varphi(\mathsf{P})$ bilden dann eine Darstellung Γ von $\mathfrak{G}$, die nicht singulär ist.

Umgekehrt gibt Schur, l. c. bei gegebenem Γ ein Verfahren um M zu konstruieren.

Nach Schur, l. c. gilt nun bei dieser Zuordnung für die Charaktere χ von Γ und Φ von M die Formel:

$$\Phi\bigl(\varphi(A)\bigr) = \sum_{\substack{\nu_1+2\nu_2+\cdots+n\nu_n=n \\ \nu_i \geqq 0}} \chi(\mathsf{P}_{\nu_1,\dots,\nu_n}) \frac{1}{\nu_1!}\left(\frac{s_1}{1}\right)^{\nu_1} \cdots \frac{1}{\nu_n!}\left(\frac{s_n}{n}\right)^{\nu_n}.$$

Dabei bezeichnet A eine Matrix aus $\mathfrak{M}$, $\varphi(A)$ ist Bild in M, $s_1, \dots, s_n$ die Potenzsummen der charakteristischen Wurzeln von A, d. h. die Spuren von $A, A^2, \dots, A^n$ und $\mathsf{P}_{\nu_1,\dots,\nu_n}$ eine Permutation aus derjenigen Klasse von $\mathfrak{G}$, deren Permutationen je ν_i Zyklen i–ten Grades haben. Man kann diese Formel, weil $\frac{n!}{\nu_1! 1^{\nu_1} \cdots \nu_n! 1^{\nu_n}}$ die Anzahl der Elemente dieser Klasse ist, auch so schreiben: VI, 67

$$\Phi\bigl(\varphi(A)\bigr) = \frac{1}{n!} \sum_{\mathsf{P} \text{ in } \mathfrak{G}} \chi(\mathsf{P}) s_1^{\nu_1(\mathsf{P})} \cdots s_n^{\nu_n(\mathsf{P})},$$

wo also $\nu_1(\mathsf{P}), \dots, \nu_n(\mathsf{P})$ die Anzahlen der Zyklen 1–ten, …, n–ten Grades von P bedeuten.

Wendet man das auf die a–reihige Einheitsmatrix $A = E_a$ an, die durch Nullen m–reihig gemacht ist (m kann ja beliebig groß sein), so entsteht wegen

$$s_1 = \cdots = s_n = a$$

*) Jede nicht homogene Darstellung ist nach Schur, l. c. reduzibel in homogene Darstellungen, deren Determinanten nicht identisch 0 sind, und eine Nulldarstellung

rechts die zu untersuchende Summe, während links eine ganze Zahl steht. Denn die charakteristischen Wurzeln von $\varphi(A)$ sind Produkte von je n der charakteristischen Wurzeln von A.

Damit ist die Formel (2) im Falle der symmetrischen Gruppe bewiesen.

3.) Für eine beliebige Gruppe $\mathfrak{G}$ ergibt sich (2) jetzt leicht, weil $\mathfrak{G}$ Untergruppe der symmetrischen Gruppe ist. Man braucht nur (2) für die symmetrische Gruppe und den durch χ_i induzierten Charakter anzusetzen.

Kapitel 7

Tagebuch VII: 1931 – 1935

Eintragungen

7.1 Maximalordnungen in einfachen Algebren und deren maximalen Teilkörpern (Mai 1931)

Comparison of the arithmetic of a central simple algebra with that of a maximal subfield. Hasse writes that he had done this investigation jointly with Artin. At the end we find a remark that later, in January 1932, Chevalley had given another proof. Chevalley's proof appeared 1934 in the "Hamburger Abhandlungen" [Che34]*. Hasse's proof appeared in the same year in the volume dedicated to the memory of Jacques Herbrand* [Has34]*. There was a third proof, by Emmy Noether, which also appeared in that memorial volume* [Noe34].

VII, 3

Im Anschluß an Untersuchungen mit Artin.

Mai 1931.

K sei eine einfache Algebra über einem algebraischen Zahlkörper Ω als Zentrum. n sei der Grad von K. k sei ein maximaler Teilkörper von K, also vom Grad n. $\mathfrak{o}$ sei eine Maximalordnung von k.

Satz 1. *Es gibt Maximalordnungen $\mathfrak{O}$ von K, die $\mathfrak{o}$ enthalten.* (Satz von Artin, Beweis von einem seiner Schüler)

Beweis. Ist $\mathfrak{O}^*$ eine beliebige Maximalordnung von K, so ist $\mathfrak{o}\mathfrak{O}^*$ Rechtsideal in $\mathfrak{O}^*$, also Linksideal in einer gewissen Maximalordnung $\mathfrak{O}$, und dabei $\mathfrak{o} \leqq \mathfrak{O}$ wegen $\mathfrak{o}.\,\mathfrak{o}\mathfrak{O}^* = \mathfrak{o}\mathfrak{O}^*$.

Satz 2. *$\mathfrak{o}$ ist dann der Durchschnitt von $\mathfrak{O}$ mit k.*

Beweis. Dieser Durchschnitt ist eine Ordnung in k, die $\mathfrak{o}$ enthält.

Satz 3. *Ist $\mathfrak{a}$ ein Ideal in $\mathfrak{o}$, so ist $\mathfrak{a}\mathfrak{Z}$ ein Rechtsideal in $\mathfrak{O}$, und zwar ein solches, dessen Linksordnung $\mathfrak{O}'$ ebenfalls $\mathfrak{o}$ enthält.* VII, 4

Dabei bezeichnet $\mathfrak{Z}$ irgendein gleichseitiges Ideal in $\mathfrak{O}$.

Beweis. Es gilt $\mathfrak{o}\mathfrak{a}\mathfrak{Z} = \mathfrak{a}\mathfrak{Z}$

Satz 4. *Ist $\mathfrak{A}$ ein Rechtsideal in $\mathfrak{O}$, prim zur Differente von $\mathfrak{O}$, dessen Linksordnung $\mathfrak{O}'$ ebenfalls $\mathfrak{o}$ enthält, so ist $\mathfrak{A}$ vom Typus $\mathfrak{a}\mathfrak{Z}$ (sogar $\mathfrak{a}$).*

Beweis. (von mir) Ich betrachte die p–Komponenten $\mathfrak{A}_p$, $\mathfrak{O}_p$, K_p, $\mathfrak{O}'_p$, $\mathfrak{o}_p$, k_p, Ω_p

für irgendein Primideal p von Ω. Nach der Voraussetzung genügt es, die in $\mathfrak{O}$ unverzweigten p zu betrachten. Für ein solches kann K_p als das System aller n–reihigen Matrizen aus Ω_p dargestellt werden. Ohne Einschränkung kann $\mathfrak{O}_p$ als das System aller ganzzahligen Matrizen aus Ω_p angenommen werden. $\mathfrak{A}_p$ ist Hauptideal in $\mathfrak{O}_p$. Sei

$$\mathfrak{A}_p = \mathsf{A}_p \mathfrak{O}_p \,.$$

VII, 5 Dann sei $\mathfrak{o}$ gleichzeitig Zeichen für eine Basiszeile von $\mathfrak{o}$, also auch von $\mathfrak{o}_p$. $\mathfrak{o}_p$ in seiner Einbettung in $\mathfrak{O}_p$ ergibt sich dann durch Bildung der Darstellung

$$\alpha_p \mathfrak{o} = \mathfrak{o} M_{\alpha_p} \qquad (\alpha_p \text{ beliebig in } \mathfrak{o}_p)$$

in Gestalt der Matrizen M_{α_p} aus Ω_p. Die Transformation auf die neue Basis $\mathfrak{o}\mathsf{A}_p$ ergibt:

$$\alpha_p \cdot \mathfrak{o}\mathsf{A}_p = \mathfrak{o}\mathsf{A}_p \cdot \mathsf{A}_p^{-1} M_{\alpha_p} \mathsf{A}_p \,.$$

Weil $\mathfrak{o} \leqq \mathfrak{O}' = \mathfrak{A}\mathfrak{O}\mathfrak{A}^{-1}$, ist $\mathfrak{o}_p \leqq \mathfrak{O}'_p = \mathfrak{A}_p\mathfrak{O}_p\mathfrak{A}_p^{-1} = \mathsf{A}_p\mathfrak{O}_p\mathsf{A}_p^{-1}$, d. h. $\mathsf{A}_p^{-1}\mathfrak{o}_p\mathsf{A}_p \leqq \mathfrak{O}_p$. Daher sind die Matrizen $\mathsf{A}_p^{-1} M_{\alpha_p} \mathsf{A}_p$ alle ganz. Das bedeutet aber, daß $\mathfrak{o}\mathsf{A}_p$ Idealbasis bezgl. $\mathfrak{o}_p$ ist. Da auch in $\mathfrak{o}_p$ jedes Ideal Hauptideal ist, gilt also:

$$\mathfrak{o}\mathsf{A}_p = \alpha_p \mathfrak{o} = \mathfrak{o} M_{\alpha_p} \text{ mit festem } \alpha_p \text{ aus } k_p \,,$$

daher

$$\mathsf{A}_p = M_{\alpha_p} \text{ aus } k_p \text{ (bei seiner Einbettung in } K_p),$$

d. h.

$$\mathfrak{A}_p = \mathfrak{a}_p \,,$$

VII, 6 wo $\mathfrak{a}_p$ ein Ideal aus k_p bezgl. $\mathfrak{o}_p$ bezeichnet.

Durch Zusammensetzung von $\mathfrak{A}$ aus seinen Komponenten ergibt sich dann die Behauptung.

Bemerkung. Chevalley (Brief vom Januar 1932) hat einen anderen Beweis für diesen Satz gegeben, und überdies gezeigt, daß der Satz *nicht* mehr allgemein gilt, wenn die Einschränkung „$\mathfrak{A}$ prim zur Differente von $\mathfrak{O}$“ aufgehoben wird.

7.2 Unmöglichkeit der Gleichung $x^5+y^5+z^5=0$. (Nov. 1931)

Dirichlet's proof [Dir28] *modernized, that the quintic Fermat equation does not have nontrivial rational solutions. Hasse had written down this for use in his seminar.*

VII, 7

Moderne Fassung von Dirichlets Beweis,
präpariert für das Seminar.

November 1931.

Fall I, x, y, z prim zu 5, erweist sich durch Betrachtung mod. 5^2 als unmöglich

Fall II, x, y prim zu 5, z durch 5 teilbar, führt nach Umbenennung auf einen der beiden Typen:

(1.) $$x^5-(\pm y)^5=(5^m z)^5 \quad \left\{\begin{array}{l} x,\ y,\ z \text{ ganzrational, positiv, prim} \\ \text{zu 5 und zueinander, } m \geqq 1\,. \end{array}\right.$$

1.) *Identität in* x, y.

$$\begin{aligned} & x^5-y^5 \\ & \quad = (x-y)\,\left[(x-\varepsilon y)(x-\varepsilon^{-1}y)\right]\,\left[(x-\varepsilon^2 y)(x-\varepsilon^{-2}y)\right] \qquad \varepsilon=e^{\frac{2\pi i}{5}} \\ & \quad = (x-y)(x^2+\omega xy+y^2)(x^2+\omega' xy+y^2) \qquad \left\{\begin{array}{c} \omega=\frac{1-\sqrt{5}}{2}\,, \\ \omega+\omega'=1\,, \\ \omega\omega'=-1\,. \end{array}\right. \end{aligned}$$

2.) *Vorbereitende Reduktion von* (1.).

$$\begin{aligned} (5^m z)^5 &= x^5-(\pm y)^5 \\ &= (x\mp y)(x^2\pm\omega xy+y^2)(x^2\pm\omega' xy+y^2) \\ &= d \quad\cdot\quad \alpha \quad\cdot\quad \alpha' \qquad \left\{\begin{array}{l} d \text{ ganzrat., pos.} \\ \alpha,\ \alpha' \text{ ganz, konj. in} \\ \mathsf{R}(\sqrt{5})\,,\text{ pos.} \end{array}\right. \end{aligned}$$

VII, 8

$$\left.\begin{array}{lcl} \alpha - d^2 & = & \mp\sqrt{5}\,\omega xy \\ \alpha' - d^2 & = & \pm\sqrt{5}\,\omega' xy \\ \alpha' - \alpha & = & \pm\sqrt{5}\,xy \end{array}\right\}\quad \begin{array}{l}(d,\,\alpha,\,\alpha') = \sqrt{5}\,, \\ \alpha, \alpha' \text{ je nur durch } \sqrt{5}^{1} \text{ teilbar.}\end{array}$$

$$\left.\begin{array}{lcl} d & = & 5^{5m-1}\,w^5 \\ \alpha & = & -\sqrt{5}\,\omega^{\nu}\xi^5 \\ \alpha' & = & \sqrt{5}\,\omega'^{\nu}\xi'^5 \end{array}\right\}$$

w ganzrat., pos., ξ, ξ' ganz, konj. in $\mathsf{R}(\sqrt{5})$, ξ' pos., w, ξ, ξ' prim zu 5 und zueinander, (ev. Einheitsfaktor -1 kann zu ξ gezogen werden).

$$\begin{array}{lcl} \alpha & \equiv & \alpha - d^2 \equiv \mp\sqrt{5}\,\omega xy \ \text{ mod. } 5^{5m-1} \\ \omega^{\nu}\xi^5 & \equiv & \pm\omega xy \ \text{ mod. } 5^{5m-2}, \text{ also mod. } 5 \\ \omega^{\nu-1} & \equiv & \text{rat. Zahl mod. } 5 \\ \nu & \equiv & 1 \text{ mod. } 5\,, \ \text{o.B.d.A. } \ \nu = 1\,. \end{array}$$

$$\left.\begin{array}{lcl} d & = & 5^{5m-1}w^5 \\ \alpha & = & -\sqrt{5}\,\omega\,\xi^5 \\ \alpha' & = & \sqrt{5}\,\omega'\,\xi'^5 \end{array}\right\}$$

w ganzrat., pos., ξ, ξ' ganz, konj. in $\mathsf{R}(\sqrt{5})$, *beide* pos., w, ξ, ξ' prim zu 5 und zueinander.

$$\left.\begin{array}{lcl|l} d^2 & = & 5^{10m-2}(w^2)^5 & -1 \\ \alpha & = & -\sqrt{5}\,\omega\,\xi^5 & \omega' \\ \alpha' & = & \sqrt{5}\,\omega'\,\xi'^5 & \omega \end{array}\right\} +$$

$$0 = -5^{10m-2}(w^2)^5 + \sqrt{5}\,\xi^5 - \sqrt{5}\,\xi'^5$$

(2.) $$\xi^5 - \xi'^5 = \left(\sqrt{5}^{\,4m-1} w^2\right)^5 = \left(\sqrt{5}^{\,2k+1} z_0\right)^5, \quad \left\{\begin{array}{lcl} w^2 & = & z_0\,, \\ 4m-1 & = & 2k+1\,. \end{array}\right.$$

VII, 9

3.) *In sich zurücklaufende Reduktion von* **(2.)**

$$\begin{array}{rcl} \left(\sqrt{5}^{\,2k+1} z_0\right)^5 & = & (\xi - \xi')(\xi^2 + \omega\xi\xi' + \xi'^2)(\xi^2 + \omega'\xi\xi' + \xi'^2) \\ & = & \delta_1 \quad\cdot\quad \alpha_1 \quad\cdot\quad \alpha_1' \end{array}$$

Wie vorher:

$$\left.\begin{array}{lcl} \delta_1 & = & \sqrt{5}^{\,10k+3} w_1^5 \\ \alpha_1 & = & -\sqrt{5}\,\omega\,\xi_1^5 \\ \alpha_1' & = & \sqrt{5}\,\omega'\,{\xi_1'}^5 \end{array}\right\}$$

w_1 ganzrat., pos., ξ_1, ξ_1' ganz, konj. in $\mathsf{R}(\sqrt{5})$, pos., w_1, ξ_1, ξ_1' prim zu 5 und zueinander.

$$(\mathbf{2_1.}) \qquad \xi_1^5 - {\xi_1'}^5 = \left(\sqrt{5}^{\,4k+1} w_1^2\right)^5 = \left(\sqrt{5}^{\,2k_1+1} z_1\right)^5, \quad \begin{cases} 4k+1 & = & 2k_1+1\,, \\ w_1^2 & = & z_1\,. \end{cases}$$

4.) *Größenabschätzung.*

$$\xi = \frac{t + s\sqrt{5}}{2}\,, \qquad \xi_1 = \frac{t_1 + s_1\sqrt{5}}{2}$$

$$\delta_1 = \xi - \xi' = s\sqrt{5} > 0\,, \qquad \delta_2 = \xi_1 - \xi_1' = s_1\sqrt{5} > 0$$

$$s > 0\,, \qquad s_1 > 0$$

$$s = \sqrt{5}^{\,10k+2} w_1^5,$$

$$s^2 = \sqrt{5}^{\,20k+4} w_1^{10} = \frac{\xi_1^5 - {\xi_1'}^5}{\sqrt{5}} \qquad = 5s_1\,\frac{t_1^4 + 10t_1^2 s_1^2 + 5s_1^4}{2^4}$$

$$2^4 s^2 = 5s_1(t_1^4 + 10t_1^2 s_1^2 + 5s_1^4) \qquad \geqq 5^2 s_1^5 \geqq 5^2 s_1^2$$

$$4^2 s^2 \geqq 5^2 s_1^2, \qquad s_1^2 \geqq \left(\frac{5}{4}\right)^2 s_1^2 > s_1^2,$$

$$s > s_1\,.$$

7.3 Beweis der Vennekohlschen Binomialkongruenzen. (Dez. 1931)

Vennekohl was a doctoral student of Hasse. He got his degree in 1931. In his thesis he gave another proof of Hasse's explicit formula for the reciprocity law with respect to an odd prime ℓ in the field of ℓ-th roots of unity. See the entry 6.4 of October 16, 1928.] While there the proof rested on the method of Eisenstein, Vennekohl used here another method based on a paper by Hensel and Hasse about local norms. In the course of the proof it was necessary to use and prove certain congruence relations for binomial coefficients. The present entry contains the proof of those relations. Vennekohl's thesis appeared 1932 [Ven32].

VII, 10

Dezember 1931.

Sie lauten:

$$G_{m,n,r} = \sum_{\mu \equiv r\ (\ell^n)} (-1)^\mu \binom{m}{\mu} \equiv 0 \text{ mod. } \ell^a \,,$$

wenn $m \geqq 0\,,\ n \geqq 1\,,\ r$ beliebige ganze Zahl, und

$$a = \left[\frac{m - \ell^{n-1}}{\varphi(\ell^n)} \right] .$$

1.) Ist ζ_n eine primitive ℓ^n–te Einheitswurzel, so hat man

$$\begin{aligned} F_{m,n,r} &= \sum_{\nu=0}^{\ell^n-1} \zeta_n^{-\nu r} (1-\zeta_n^\nu)^m = \sum_{\nu=0}^{\ell^n-1} \zeta_n^{-\nu r} \sum_\mu (-1)^\mu \binom{m}{\mu} \zeta_n^{\nu\mu} \\ &= \sum_\mu (-1)^\mu \binom{m}{\mu} \sum_{\nu=0}^{\ell^n-1} \zeta_n^{-\nu(\mu-r)} = \ell^\nu \sum_{\mu \equiv r\ (\ell^n)} (-1)^\mu \binom{m}{\mu} \\ &= \ell^\nu G_{m,n,r} \,. \end{aligned}$$

Es genügt also zu zeigen:

$$F_{m,n,r} = \sum_{\nu=0}^{\ell^n-1} \zeta_n^{-\nu r} (1-\zeta_n^\nu)^m \equiv 0 \text{ mod. } \ell^{a+\nu}.$$

2.) Bezeichnet $S_n(\ldots)$ die Spur im Körper K_n der ℓ^n–ten Einheitswurzeln, so ergibt sich durch Zerlegung der $\sum\limits_{\nu}$ nach $(\nu,\, \ell^n)$: VII, 11

$$F_{m,n,r} = S_n(\zeta_n^{-r}\lambda_n^m) + S_{n-1}(\zeta_{n-1}^{r}\lambda_{n-1}^m) + \cdots + S_1(\zeta_1^{-r}\lambda_1^m)\,.$$

Dabei ist $\lambda_n = 1 - \zeta_n$ der Primteiler von ℓ in K_n. Es kommt also auf die Untersuchung von $S_n(\zeta_n^{-r}\lambda_n^m)$ an.

3.) Nun ist

$$S_n(\zeta_n^{-r}\lambda_n^m) = S_n(\ell^a\lambda_1\gamma_n)$$

mit ganzem γ_n aus K_n, weil $m \geqq a\varphi(\ell^n)+\ell^{n-1}$ nach Definition von a. Zunächst ist die Relativspur $S_{n1}(\ldots)$ in bezug auf K_1:

$$S_{n1}(\zeta_n^{-r}\lambda_n^m) = S_{n1}(\ell^a\lambda_1\gamma_n) = \ell^a\lambda_1 S_{n1}(\gamma_n) \equiv 0 \ \text{mod.}\ \ell^{a+n-1}\lambda_1\,.$$

Denn es ist

$$S_{n1}(\gamma_n) \equiv 0 \ \text{mod.}\ \ell^{n-1},$$

weil die Relativdifferente von K_n/K_{n-1} nach der Theorie der Kummerschen Körper $\sim \ell$ ist, also die Relativdifferente von $K_n/K_1 \sim \ell^{n-1}$.

Setzt man dementsprechend

$$S_{n1}(\zeta_n^{-r}\lambda_n^m) = \ell^{a+n-1}\lambda_1\gamma_1$$

mit ganzem γ_1 aus K_1, so folgt: VII, 12

$$S_n(\zeta_n^{-r}\lambda_n^m) = S_1\big(S_{n1}(\zeta_n^{-r}\lambda_n^m)\big) = \ell^{a+n-1}S_1(\lambda_1\gamma_1) \equiv 0 \ \text{mod.}\ \ell^{a+n}.$$

Beachtet man, daß

$$\begin{aligned} m \geqq a\varphi(\ell^n) + \ell^{n-1} \ &\geqq\ a\ell\varphi(\ell^n) + \ell^{n-2} \geqq \cdots \\ &\geqq\ a\ell^{n-1}\varphi(\ell) + 1\,, \end{aligned}$$

so folgt hieraus:

$$\begin{array}{rcll} S_{n-1}(\zeta_{n-1}^{-r}\lambda_{n-1}^m) & \equiv & 0 \ \text{mod.}\ \ell^{a\ell+n-1}, & \text{also sicher mod.}\ \ell^{a+n} \\ \cdots\cdots & \cdots & \cdots\cdots & \cdots\cdots \\ S_1(\zeta_1^{-r}\lambda_1^m) & \equiv & 0 \ \text{mod.}\ \ell^{a\ell^{n-1}+1}, & \text{also sicher mod.}\ \ell^{a+n} \end{array}$$

Nach obigem ergibt sich jetzt in der Tat:

$$F_{m,n,r} \equiv 0 \ \text{mod.}\ \ell^{a+n}.$$

7.4 Davenport's Beweis der Lösbarkeit von $ax^m + by^n + c \equiv 0 \mod p$ und Bestimmung der Anzahl der Lösungen.

This entry shows that Hasse had become interested, through Davenport, in solutions of congruences modulo a prime, which was the motivation of Hasse's later work on the Riemann Hypothesis for curves over finite fields. The entry is not dated but the evidence points towards January 1932. Davenport had visited Hasse in early January 1932. At that occasion Hasse had asked Davenport for the detailed proof. The present entry is a precise copy of Davenport's letter which he had sent Hasse immediately after his return to Cambridge. At the end of the entry Hasse mentions another proof by Mordell. The latter had visited Hasse at the end of January 1932. Mordell's proof appeared 1933 in the "Mathematische Zeitschrift" [Mor33]. *See also* [Roq04, Roq12].

VII, 13

Ohne Einschränkung seien m und n Teiler von $p-1$. Seien $\chi_1, \ldots, \chi_{m-1}$ bzw. $\psi_1, \ldots, \psi_{n-1}$ die vom Hauptcharakter verschiedenen m–ten bzw. n–ten Potenzrestcharaktere mod. p. Da dann die Kongruenz $x^m \equiv t$ mod. p genau $1 + \chi_1(t) + \cdots + \chi_{m-1}(t)$ Lösungen hat, und entsprechend für n, folgt für die Lösungsanzahl N der zu untersuchenden Kongruenz:

$$N = \sum_t \{1 + \chi_1(t) + \cdots + \chi_{m-1}(t)\}\Big\{1 + \psi_1\left(-\frac{at+c}{b}\right) + \cdots \\ \cdots + \psi_{n-1}\left(-\frac{at+c}{b}\right)\Big\},$$

wo die Summe, wie alle folgenden unbezeichneten Summen, über ein volles Restsystem mod. p zu erstrecken ist.

Hieraus folgt:

$$N = p + \sum_{r=1}^{m-1}\sum_{s=1}^{n-1}\sum_t \chi_r(t)\psi_s\left(-\frac{at+c}{b}\right).$$

Die $\sum_t$ kann nun leicht durch verallgemeinerte Gaussche Summen

$$\tau(\chi) = \sum_\mu \chi(\mu) e^{\frac{2\pi i\mu}{p}}$$

ausgedrückt werden. Diese haben ja die Eigenschaft: VII, 14

$$\overline{\chi}(u)\tau(\chi) = \sum_{\mu} \chi(\mu) e^{\frac{2\pi i u\mu}{p}}.$$

Daraus folgt:

$$\begin{aligned}\sum_{t} \chi(t)\psi(at+c) &= \frac{1}{\tau(\overline{\psi})} \sum_{t,\nu} \chi(t)\, e^{\frac{2\pi i(at+c)\nu}{p}}\, \overline{\psi}(\nu) \\ &= \frac{\tau(\chi)}{\tau(\overline{\psi})} \sum_{\nu} \overline{\chi}(a\nu)\overline{\psi}(\nu)\, e^{\frac{2\pi i c\nu}{p}} \\ &= \frac{\tau(\chi)\tau(\overline{\chi}\,\overline{\psi})}{\tau(\overline{\psi})}\, \overline{\chi}(a)\, \chi\psi(c)\,.\end{aligned}$$

Daher ist

$$N = p + \sum_{r=1}^{m-1} \sum_{s=1}^{n-1} \frac{\tau(\chi_r)\tau(\overline{\chi}_r\overline{\psi}_s)}{\tau(\overline{\psi}_s)}\, \chi_r\left(\frac{c}{a}\right)\psi_s\left(-\frac{c}{b}\right).$$

Da $|\tau| = \sqrt{p}$, folgt also:

$$N = p + \vartheta\sqrt{p}\,(m-1)(n-1) \qquad \text{mit} \ \ |\vartheta| \leqq 1$$

Insbesondere:

$$N > 0\,, \ \text{wenn} \ \ p > (m-1)^2(n-1)^2.$$

Bemerkung. Siehe auch den Mordellschen Beweis, der zwar ein nicht ganz so scharfes Resultat liefert, aber dafür frei von Gaussschen Summen, somit völlig elementar ist. (Eingereicht bei der Math. Zeitschr. im März 1932.)

7.5 Hardy–Littlewoodscher Beweis des Primzahlsatzes nach Landau. (Feb. 1932)

The proof of the prime number theorem due to Hardy and Littlewood, given by Landau. The meaning of the reference to Landau is not known. Perhaps Hasse, who visited Göttingen in the days February 29–March 2, 1932, had a conversation with Landau there. Or maybe he extracted this proof from Landau's book on prime numbers.

VII, 15

Februar 1932.

Der Primzahlsatz ergibt sich in der gewohnten, elementaren Weise, wenn nur der folgende Satz bekannt ist (der dann auf $f(s) = -\frac{\zeta'}{\zeta}(s) - \zeta(s) = \sum_{m,p} \frac{\log p}{p^{ms}} - \sum_n \frac{1}{n^s}$ anzuwenden ist):

Satz. *Sei*

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

eine für $\sigma > 1$ konvergente Dirichletsche Reihe mit reellen Koeffizienten $a_n \geqq -1$, und sei

$$f(s) = O\left(e^{|t|}\right) \quad \text{gleichmäßig für} \quad \sigma > 1\,,$$

sowie

$$f(s) \text{ regulär auf } \sigma = 1$$

(*oder auch nur* $\lim\limits_{\sigma \to 1+0} f(s)$ *gleichmäßig auf jeder festen t–Strecke vorhanden*).

Dann gilt

$$\sum_{n \leqq x} a_n = o(x)\,.$$

Beweis. Für $y > 0$ und $\delta > 0$ gilt

$$e^{-y} = \frac{1}{2\pi i} \int\limits_{1+\delta-i\infty}^{1+\delta+i\infty} y^{-s}\, \Gamma(s)\, ds\,.$$

(Der Beweis dieser Mellinschen Formel wird am einfachsten durch Differenzieren erbracht.) VII, 16

Durch Anwendung dieser Formel folgt in gewohnter Weise:

$$\sum_{n=1}^{\infty} a_n e^{-ny} = \frac{1}{2\pi i} \int_{(1+\delta)} y^{-s}\,\Gamma(s) f(s)\,ds\,,$$

$$\left(\begin{array}{c}\text{Zur Konvergenz beachte man:}\\ \Gamma(s) = O\left(e^{-\frac{\pi}{2}|t|}\,|t|^c\right)\end{array}\right)$$

also

$$y\sum_{n=1}^{\infty} a_n e^{-ny} = \frac{1}{2\pi i} \int_{(1+\delta)} y^{1-s}\,\Gamma(s) f(s)\,ds$$

Nach der Voraussetzung über $f(s)$ kann der Integrationsweg bis zur Geraden (1) verschoben werden:

$$\begin{aligned} y\sum_{n=1}^{\infty} a_n e^{-ny} &= \frac{1}{2\pi i} \int_{(1)} y^{1-s}\,\Gamma(s) f(s)\,ds \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{it\log\frac{1}{y}}\,\Gamma(s) f(s)\,dt \qquad (s = 1+it) \end{aligned}$$

Rechts die Fourier–Konstante einer absolut integrabeln Funktion $\Gamma(s)f(s)$ vor, die bekanntlich für $\log\frac{1}{y} \to \infty$, dh. $y \to 0$ zu 0 strebt.
Es ist also

$$y\sum_{n=1}^{\infty} a_n e^{-ny} = o(1) \quad \text{für} \quad y \to 0\,.$$

Nach dem Satz von Karamata folgt daraus

$$\sum_{n \leqq x} a_n = o(m) \quad \text{für} \quad x \to \infty\,.$$

7.6 Verschärfung eines Satzes von Minkowski nach Landau. (Feb. 1932)

A lower bound for the non-zero values of a binary quadratic form with discriminant 1 is given by $\frac{1}{\sqrt{5}}$.

VII, 17

Februar 1932.

Es sei $f(x,y) = ax^2 + bxy + cy^2$ eine reelle quadratische Form der Diskriminante $b^2 - 4ac = 1$. Es handelt sich um die untere Grenze

$$p = p(f) = p(a,b,c)$$

der Werte von f für ganzzahlige $x, y \neq 0, 0$.

Satz. *Es ist* $p \leqq \dfrac{1}{\sqrt{5}}$.

Beweis. $p(f)$ hängt nur von der arithmetischen Klasse von f ab (ganzzahlige Substitutionen der Determinante ± 1) und ist auch für $\pm f$ dasselbe. Daher kann ohne Einschränkung vorausgesetzt werden, daß a irgendeine positive, eigentlich (mit teilerfremden ganzen x, y) durch f darstellbare Zahl ist. Nach der Definition von p kann insbesondere für a eine beliebig nahe oberhalb p gelegene Zahl vorgeschrieben werden.

VII, 18

Wir schreiben vor:

$$p \leqq a < \sqrt{p^2 + \frac{1}{4}}\,.$$

Ferner kann b mod. $2a$ beliebig abgeändert werden.
Wir schreiben vor:

$$-2a + \sqrt{1 + 4ap} \leqq b < \sqrt{1 + 4ap}\,.$$

Um hieraus eine beiderseitige Abschätzung für

$$c = \frac{b^2 - 1}{4a}$$

herzuleiten, weisen wir zunächst nach, daß die untere für b festgesetzte Schranke

$$-2a + \sqrt{1 + 4ap} > 0$$

ist. In der Tat ist nach der Vorschrift über a:

$$2a < \sqrt{1+4p^2} \leqq \sqrt{1+4ap}\,.$$

Unter Berücksichtigung dieser Tatsache folgt jetzt einerseits:

$$c < p\,,$$

andrerseits:

$$c \geqq \frac{\left(-2a+\sqrt{1+4ap}\right)^2 - 1}{4a} = a + p - \sqrt{1+4ap}\,.$$

Daß hiernach VII, 19

$$c > -p$$

ist, folgt rückwärts aus der Kette:

$$\begin{aligned} a + p - \sqrt{1+4ap} &> -p \\ a + 2p &> \sqrt{1+4ap} \\ a^2 + 4p^2 &> 1 \\ 5p^2 &> 1\,, \end{aligned}$$

wenn nur die letztere Relation gilt.

Da $c > -p$ einen Widerspruch mit der Definition von p ergäbe (nämlich $|f(0,1)| = |c| < p$), muß notwendig

$$a + p - \sqrt{1+4ap} \leqq -p$$

sein. Das ergibt weiter:

$$\begin{aligned} a + 2p &\leqq \sqrt{1+4ap} \\ a^2 + 4p^2 &\leqq 1 \\ 5p^2 &\leqq 1 \\ p &\leqq \frac{1}{\sqrt{5}}\,. \end{aligned}$$

Bemerkung. Für $f(x,y) = \frac{x^2+xy-y^2}{\sqrt{5}}$ ist ersichtlich $p = \frac{1}{\sqrt{5}}$. Die Abschätzung des Satzes ist also die bestmögliche für alle f gültige.

7.7 Modifikation des Beweises von $h \geqq n$ in der Theorie der zyklischen Körper. (März 1932)

This entry is written after Artin's celebrated lectures in Göttingen (February 29–March 2, 1932). Hasse had attended these lectures. Artin had presented the new foundation of class field theory which had been recently achieved with ideas from Herbrand, Chevalley and himself. Lecture notes were prepared by Olga Taussky and distributed among the interested people. (*Years later they appeared in print* [Coh78].) *In one of the footnotes of those lecture notes it is mentioned that in the meantime Hasse had found a new short proof of one of the two main inequalities of class field theory: $h \geq n$. Here we find that new proof. On the last page of the present entry Hasse refers to a letter from Artin of May 2, 1932. For this see* [FR08]. *The ideas of this entry found their way into Hasse's "Marburg lectures" on class field theory* [Has33b].

VII, 20

März 1932.

K sei ein zyklischer Körper vom Grade n über dem algebraischen Zahlkörper k. Es sei S eine erzeugende Substitution für K/k und

$$\begin{aligned} N &= 1 + \mathsf{S} + \cdots + \mathsf{S}^{n-1} \quad \text{(Norm)} \\ \Delta &= 1 - \mathsf{S} \end{aligned}$$

Es möge durchweg die Gleichheit für Ideale in dem modifizierten Sinne verstanden werden, daß Primteiler des Führers $\mathfrak{f}$ von K/k als 1 gelten. Entsprechend ist der Begriff der Einheit zu modifizieren. $\mathfrak{f}$ ist dabei als das Produkt der $\mathfrak{p}$–Führer $\mathfrak{f}_{\mathfrak{p}}$ gemeint.

Wir betrachten den Quotienten

$$q = \frac{\left[\mathfrak{a} : \mathfrak{A}^N(\nu)\right]}{\left[\nu \cap \mathfrak{A}^N : \mathsf{A}^N\right]} = \frac{h}{s}$$

$\mathfrak{a}$ Ideale aus k
$\mathfrak{A}$ Ideale aus K
A Zahlen aus K
ν Normenreste mod. $\mathfrak{f}$ von K in k.

(NB. Es ist keinerlei Bedingung „prim zu $\mathfrak{f}$" gestellt.) Der Zähler von q ist offenbar der Index der Takagischen Gruppe mod. $\mathfrak{f}$ von K in k, während der Nenner die Abweichung von der Gültigkeit des Normensatzes für K/k mißt.

VII, 21

Erste Umformungsserie (Abspaltung der Klassenkörpertheorie im Kleinen)

$$
\begin{aligned}
q &= \frac{\left[\mathfrak{a} : \mathfrak{A}^N(\nu)\right]}{\left[\nu \cap \mathfrak{A}^N : \mathsf{A}^N\right]} \\
&= \frac{[\mathfrak{a} : (\nu)]}{[\mathfrak{A}^N(\nu) : (\nu)]\ [(\nu) \cap \mathfrak{A}^N : (\mathsf{A}^N)]\ [\nu \cap \varepsilon : \Theta^N]}
\end{aligned}
$$

ε Einheiten aus k
Θ Zahlen aus K, für die Θ^N Einheit

$$
\begin{aligned}
&= \frac{[\mathfrak{a} : (\nu)]}{[\mathfrak{A}^N : (\mathsf{A})^N]\ [\nu \cap \varepsilon : \Theta^N]} \\
&= \frac{[\mathfrak{a} : (\alpha)]\ [(\alpha) : (\nu)]}{[\mathfrak{A}^N : (\mathsf{A})^N]\ [\nu \cap \varepsilon : \Theta^N]} \\
&= \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N]\ [\varepsilon : \nu \cap \varepsilon]\ [\nu \cap \varepsilon : \Theta^N]}\ [\alpha : \nu] \\
&= \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N]\ [\varepsilon : \Theta^N]}\ [\alpha : \nu] = q_0 \cdot [\alpha : \nu] \\
&= q_0 \cdot \prod_{\mathfrak{p} | f} n_{\mathfrak{p}}\,,
\end{aligned}
$$

wo $n_{\mathfrak{p}}$ den $\mathfrak{p}$–Grad von K/k (Grad von $K_{\mathfrak{P}}/k_{\mathfrak{p}}$) bezeichnet, während q_0 der verbleibende Ausdruck ist.

Zweite Umformungsserie (Theorie der ambigen Klassen).

VII, 22

$$
\begin{aligned}
\left[\mathfrak{A}^N : (\mathsf{A})^N\right] &= \left[\mathfrak{A} : \mathfrak{A}^\Delta(\mathsf{A})\right] \\
&= \frac{[\mathfrak{A} : (\mathsf{A})]}{[\mathfrak{A}^\Delta(\mathsf{A}) : (\mathsf{A})]} \\
&= \frac{[\mathfrak{A} : (\mathsf{A})]}{[\mathfrak{A} : \mathfrak{B}]} \\
&= [\mathfrak{B} : (\mathsf{A})]
\end{aligned}
$$

$\mathfrak{B}$ Ideale aus K, für die $\mathfrak{B}^\Delta$ Hauptideal (ambige Klassen).

Dritte Umformungsserie (Berechnung der Anzahl der ambigen Klassen).

$$
\begin{aligned}
[\mathfrak{B} : (\mathsf{A})] &= \big[(\Theta) : (\mathsf{A}^{\Delta})\big]\ [\mathfrak{a} : (\mathsf{B})] \\
&= \big[\Theta : \mathsf{A}^{\Delta}\mathsf{E}\big]\ \frac{[\mathfrak{a} : (\alpha)]}{[\mathsf{B} : \alpha\mathsf{E}]} \\
&= \frac{\big[\Theta^N : \mathsf{E}^N\big]}{[\mathsf{H} : \mathsf{E}^{\Delta}]}\ [\mathfrak{a} : (\alpha)]
\end{aligned}
$$

B Zahlen aus K, für die (B) Ideal ist

E Einheiten in K

H Einheiten in K, für die $\mathsf{H}^N = 1$.

VII, 23

Resultat der zweiten und dritten Umformungsserie für den Restfaktor q_0

$$
\begin{aligned}
q_0 &= \frac{[\mathfrak{a} : (\alpha)]}{[\mathfrak{A}^N : (\mathsf{A})^N]\ [\varepsilon : \Theta^N]} \\
&= \frac{\big[\mathsf{H} : \mathsf{E}^{\Delta}\big]}{[\varepsilon : \Theta^N]\ [\Theta^N : \mathsf{E}^N]} = \frac{\big[\mathsf{H} : \mathsf{E}^{\Delta}\big]}{[\varepsilon : \mathsf{E}^N]}
\end{aligned}
$$

Wird dieser Quotient mittels des Herbrandschen Übergangssatzes zu einer Untergruppe, und durch Konstruktion einer geeigneten (regulären) Einheitenbasis nach dem Schema von Minkowski–Herbrand–Artin, zu

$$q_0 = \frac{n}{\prod\limits_{\mathfrak{p}|f} n_{\mathfrak{p}}}$$

berechnet*), so folgt also:

$$q = n\,.$$

Dies bedeutet:

$$h = n \cdot s\,.$$

Die Analysis ergibt aber

$$h \leqq n\,.$$

Kombination gibt $h = n$ (K/k ist Klassenkörper mod. f) und $s = 1$ (Normensatz).

*) Siehe dazu Brief von Artin vom 2. Mai 1932

7.8 Davenport's Abschätzung der kubischen Exponentialsummen. (Apr. 1932)

This is a reproduction of Davenport's proof which Hasse had accepted for Crelle's Journal; see [Dav33]. *At the end of this entry we find another proof, this time of Mordell, which however yields only the estimate $p^{3/4}$ whereas Davenport had improved it to $p^{5/8}$. Such estimates were considered as a step towards the best estimate $p^{1/2}$ given by the Riemann hypothesis for function fields which was not yet known at the time.*

VII, 24

April 1932

Satz. *Für jedes kubische Polynom mit ganzen Koeffizienten $f(x)$ gilt*

$$\sum_x e\big(f(x)\big) = O\left(p^{\frac{5}{8}}\right) ,$$

wenn $e(t) = e^{\frac{2\pi i t}{p}}$, p eine Primzahl, und $\sum_x$ die Summe über ein volles Restsystem mod. *p bezeichnet.*

Beweis. O. B. d. A. (Parallelverschiebung von x) sei

$$f(x) = ax^3 + cx ,$$

ferner $p \geqq 5$.
Wir setzen

$$\mathsf{S}_{a,c} = \sum_x e(ax^3 + cx) .$$

Dann ist

$$\begin{aligned}
|\mathsf{S}_{a,c}|^2 &= \sum_{x,y} e(ay^3 - ax^3 + cy - cx) \\
&= \sum_{x,t} e(at^3 + 3axt^2 + 3ax^2t + ct) \qquad (y = x + t) \\
&= \sum_{x',t} e(3atx'^2 + \frac{1}{4}\,at^3 + ct) \qquad \left(x = x' - \frac{1}{2}\,t\right) \\
&= p + {\sum_t}' e\left(\frac{1}{4}\,at^3 + ct\right) i^{\left(\frac{p-1}{2}\right)^2} \sqrt{p} \left(\frac{3at}{p}\right) \qquad \left(\begin{array}{l}\text{Auswertung der} \\ \text{Gausschen Summe}\end{array}\right) \\
&= p + \varepsilon\, \mathsf{R}_{b,c} \sqrt{p}\,, \quad {}^{1}
\end{aligned}$$

VII, 25

wo $|\varepsilon| = 1$ und

$$\mathsf{R}_{b,c} = \sum_t \left(\frac{t}{p}\right) e(bt^3 + ct) \qquad \left(b = \frac{a}{4}\right)\,.$$

Erste Methode zur Abschätzung von $\mathsf{R}_{b,c}$.

$$\begin{aligned}
|\mathsf{R}_{b,c}|^2 &= \sum_{x,y} \left(\frac{xy}{p}\right) e(by^3 - bx^3 + cy - cx) \\
& \qquad\qquad\qquad\qquad\qquad\qquad (y = x + t) \\
&= \sum_{x,t} \left(\frac{x(x+t)}{p}\right) e(bt^3 + 3bt^2x + 3btx^2 + ct) \\
& \qquad\qquad\qquad\qquad\qquad\qquad (x = ut) \\
&= p - 1 + {\sum_t}' \sum_u \left(\frac{u(u+1)}{p}\right) e\big(b(1 + 3u + 3u^2)t^3 + ct\big) \\
&< p + \sum_u \left| \sum_t e\big\{b(1 + 3u + 3u^2)t^3 + ct\big\} \right| \\
&< p + 2 \sum_v \left| \sum_t e(vt^3 + ct) \right|
\end{aligned}$$

[1] Hasse writes erroneouly $t + \cdots$ instead of $p + \cdots$.

Nun ist

$$\sum_v \Big| \sum_t e(vt^3+ct) \Big|^2 = p \sum_{t_1^3 \equiv t_2^3\,(p)} e\big\{c(t_2-t_1)\big\} \qquad \text{(Mordell's Methode)}\,,$$

$$\text{also} < 3p^2,$$

somit nach der Schwarzschen Ungleichung

$$|\mathsf{R}_{b,c}|^2 < p + 2\sqrt{p \cdot \sum_v \Big| \sum_t \Big|^2} < p + 2\sqrt{3p^3} = O\left(p^{\frac{3}{2}}\right)$$

Hieraus folgt: VII, 26

$$\begin{aligned} \mathsf{R}_{b,c} &= O\left(p^{\frac{3}{4}}\right) \\ \mathsf{S}_{a,c}^2 &= O\left(p^{\frac{5}{4}}\right) \\ \mathsf{S}_{a,c} &= O\left(p^{\frac{5}{8}}\right)\,. \end{aligned}$$

Zweite Methode zur Abschätzung von $\mathsf{R}_{b,c}$.

(Direkte Anwendung von Mordell's Methode)

$$\sum_{b,c} |\mathsf{R}_{b,c}|^4 = p^2 \sum_{\substack{x+y\,\equiv\, u+o \\ x^3+y^3\,\equiv\, u^3+o^3}\Big\}\,(p)} 1 = O\left(p^4\right)\,.$$

Nun

$$|\mathsf{R}_{b,c}| = |\mathsf{R}_{\lambda^3 b,\lambda c}| \qquad \lambda \not\equiv 0 \ (p)\,.$$

Daher

$$p \sum_{b,c}{}' |\mathsf{R}_{b,c}|^4 = O\left(p^4\right)\,,$$

wo $\sum'_{b,c}$ nur über nicht in der genannten Weise zusammenhängende Paare b, c erstreckt ist.

Hieraus

$$\begin{aligned} \mathsf{R}_{b,c}^4 &= O\left(p^3\right) \\ \mathsf{R}_{b,c} &= O\left(p^{\frac{3}{4}}\right)\,, \end{aligned}$$

und dann weiter wie oben.

7.9 Existenz einer regulären Basis für normale Erweiterungen 1. Art. (Apr. 1932)

Deuring's proof of the existence of normal basis was the first which worked in both cases, regardless of whether the base field is finite or infinite [Deu32]. *In his proof Deuring, who was a student of Emmy Noether, had used the terminology of algebras, or "hypercomplex systems" in the terminology of the time. The present entry uses essentially the same ideas but without explicitly referring to the theory of algebras. Later, in the entry 7.30 of February 1934, there is another proof on the existence of normal bases.]*

VII, 27

Aus einem hyperkomplexen Beweis
von Deuring destilliert.

April 1932.

Satz. *Ist K eine normale Erweiterung 1. Art von k von endlichem Grad, so existiert stets eine k–Basis von K, deren Elemente aus einem von ihnen durch Anwendung aller Automorphismen von K/k entstehen (sog. reguläre Basis).*

Beweis. Sei $(\omega_i) = \mathfrak{o}$ eine beliebige k–Basis von K und

$$\omega_i^{\mathsf{S}} = \sum_k a_{ik,\mathsf{S}} \omega_k \,, \text{ kurz } \mathfrak{o}^{\mathsf{S}} = A_{\mathsf{S}} \mathfrak{o} \,,$$

ihr Verhalten bei den Automorphismen S von K/k. Bezeichnen auch X, Y solche Automorphismen, so folgt

$$\omega_i^{\mathsf{S}Y} = \sum_k a_{ik,\mathsf{S}} \omega_k^Y \,,$$

also

$$\Omega\, P_{\mathsf{S}} = A_{\mathsf{S}} \Omega \,,$$

wo

$$\Omega = (\omega_i^Y) \,, \quad P_{\mathsf{S}} = (e_{X,\mathsf{S}Y})$$

VII, 28 Da $|\Omega| \neq 0$ (Erweiterung 1. Art), folgt die Ähnlichkeit der Darstellung A_{S} der galoisschen Gruppe von K/k mit der Permutationsdarstellung P_{S}, d. i. die reguläre Darstellung.

Bezeichnet W eine Matrix *in* k mit der Eigenschaft

$$WP_{\mathsf{S}} = A_{\mathsf{S}}W$$

und $|W| \neq 0$, wie sie in bekannter Weise aus der Existenz von Ω in K folgt *), so ist

$$\mathfrak{r} = W^{-1}\mathfrak{o}$$

eine reguläre Basis. Denn

$$\begin{aligned} \mathfrak{r}^{\mathsf{S}} &= W^{-1}\mathfrak{o}^{\mathsf{S}} = W^{-1}A_{\mathsf{S}}\mathfrak{o} = W^{-1}A_{\mathsf{S}}W\mathfrak{r} \\ &= P_{\mathsf{S}}\mathfrak{r}\,. \end{aligned}$$

7.10 Elementarer Beweis des Artinschen Lemmas in der Klassenkörpertheorie. (Apr. 1932)

Artin had used a certain lemma in his proof of his general reciprocity law [Art27]. *Chevalley in his thesis* [Che33b] *has given an elementary proof, not using class field theory. Chevalley's proof is still be simplified here by using arguments of Vandiver and Birkhoff. In the summer of 1932 Hasse included this proof in his Marburg lectures on class field theory* [Has33b], Satz (139). *See also the entries 7.18 of June 8, 1932] and 7.22 of Oktober 1932.] In the entry 7.14 of May 1932 Hasse uses Satz 1 from here.]*

VII, 29

Vereinfachung des von Chevalley
gebrachten Beweises, der sich auf
Sätze von Vandiver und Birkhoff stützt.

April 1932

Satz 1. *Es sei $a > 1$ eine natürliche Zahl und p^ν eine Primzahlpotenz. Dann existiert stets eine Primzahl q, sodaß a mod. q den Exponenten p^ν hat.*

Beweis. q ist so zu wählen, daß zwar $q | a^{p^\nu} - 1$, aber $q \nmid a^{p^{\nu-1}} - 1$ ist. Wir betrachten dazu

$$f_\nu(a) = \frac{a^{p^\nu} - 1}{a^{p^{\nu-1}} - 1}$$

und stellen fest: Falls nur $\nu \geqq 2$ für $a \equiv 1(2)$ $p = 2$, ist $f_\nu(a)$ genau durch p^0 oder p^1 teilbar.

Andrerseits ist

$$f_\nu(a) = a^{(p-1)p^{\nu-1}} + \cdots + a^{p^{\nu-1}} + 1 > p\,, \quad \text{weil} \;\; a > 1\,.$$

VII, 30 Daher hat $f_\nu(a)$ Primteiler $q \neq p$. Jeder solche genügt.

Satz 2. (Artinsches Lemma). *Es seien $a > 1$ und n natürliche Zahlen. Dann existiert stets eine zyklische Kongruenzklasseneinteilung der ganzen Zahlen, bei der a den Exponenten n hat.*

Beweis. Es sei $n = \prod_i p_i^{\nu_i}$. Dann existieren nach Satz 1 Primzahlen q_i derart, daß a mod. q_i den Exponenten $p_i^{\nu_i}$ hat.
Ist $q_i - 1$ genau durch $p_i^{\nu_i + \kappa_i}$ teilbar, und bezeichnet P_i die Gruppe der $p_i^{\nu_i+\kappa_i}$–ten Potenzreste mod. q_i, so hat a auch in bezug auf P_i den Exponenten $p_i^{\nu_i}$. In

bezug auf den Durchschnitt P aller P_i hat dann a den Exponenten $n = \prod_i p_i^{\nu_i}$, und dieser Durchschnitt P führt zu einer zyklischen Kongruenzklasseneinteilung (mod. m, wo $m = \prod_i q_i$) (der Ordnung $\prod_i p_i^{\nu_i+\kappa_i}$).

7.11 Fast reeller Beweis der Riemannschen Funktionalgleichung. (Mai 1932)

Proof of the functional equation of the Riemann zeta function according to Landau. Hasse had visited Göttingen in February 1932. We do not know whether Landau had told him about this proof, or Hasse had extracted this proof from a publication of Landau. See also 7.13.]

VII, 31

Nach Landau, Mai 1932

Satz 1. $f(s) = \int\limits_0^1 x^{s-1}\left(\frac{1}{e^x-1} - \frac{1}{x} + \frac{1}{2}\right)dx + \int\limits_1^\infty \frac{x^{s-1}}{e^x-1}\,dx$ ist für $\sigma > -1$ regulär.

Beweis. Klar, da $\frac{1}{x} - \frac{1}{2}$ der Hauptteil von $\frac{1}{e^x-1}$.

Satz 2. Für $s > 1$ ist

$$f(s) - \frac{1}{2s} + \frac{1}{s-1} = \Gamma(s)\zeta(s)$$

Beweis.

$$\begin{aligned}
\Gamma(s)\zeta(s) = \sum_{n=1}^\infty \frac{\Gamma(s)}{n^s} &= \sum_{n=1}^\infty \int\limits_0^\infty x^{s-1}e^{-nx}dx = \int\limits_0^\infty \sum_{n=1}^\infty x^{s-1}e^{-nx}dx \\
&= \int\limits_0^\infty \frac{x^{s-1}}{e^x-1}\,dx = f(s) + \int\limits_0^1 x^{s-2}dx - \frac{1}{2}\int\limits_0^1 x^{s-1}dx \\
&= f(s) + \frac{1}{s-1} - \frac{1}{2s}
\end{aligned}$$

Satz 3. Für $-1 < s < 0$ ist

$$f(s) - \frac{1}{2s} + \frac{1}{s-1} = \frac{(2\pi)^s}{2}\,\frac{1}{\cos\frac{\pi s}{2}}\,\zeta(1-s)\,.$$

Beweis.

$$\frac{(2\pi)^s}{2}\,\frac{1}{\cos\frac{\pi s}{2}}\,\zeta(1-s)=\sum_{n=1}^{\infty}\frac{(2\pi)^s}{2}\,\frac{1}{\cos\frac{\pi s}{2}}\,n^{s-1}$$

$$=\sum_{n=1}^{\infty}\int_0^{\infty}x^{s-1}\,\frac{2x}{4\pi^2n^2+x^2}\,dx \qquad \text{(siehe folgenden Hilfssatz)}$$

$$=\int_0^{\infty}x^{s-1}\sum_{n=1}^{\infty}\frac{2x}{4\pi^2n^2+x^2}\,dx=\int_0^{\infty}x^{s-1}\left(\frac{1}{e^x-1}-\frac{1}{x}+\frac{1}{2}\right)dx$$

$$=f(s)-\int_1^{\infty}x^{s-2}dx+\frac{1}{2}\int_1^{\infty}x^{s-1}dx=f(s)+\frac{1}{s-1}-\frac{1}{2s}\,.$$

Uralter Hilfssatz. Für $a>0,\ \lambda>0\,,$ VII, 32

$$\varphi(\lambda)=\int_0^{\infty}e^{-\lambda(u+1)}\,\frac{u^{a-1}}{1+u}\,du\,,\quad \psi(\lambda)=\Gamma(a)\int_{\lambda}^{\infty}e^{-u}u^{-a}du$$

ist

$$\varphi(\lambda)=\psi(\lambda)\,.$$

Beweis. $\varphi'(\lambda)=-\int_0^{\infty}e^{-\lambda(u+1)}u^{a-1}du=-e^{-\lambda}\lambda^{-a}\,\Gamma(a)=\psi'(\lambda)$

$$\varphi(\lambda)-\psi(\lambda)=\varphi(\infty)-\psi(\infty)=0\,.$$

Folgerung 1. Für $0<a<1$ ist

$$\int_0^{\infty}\frac{u^{a-1}}{1+u}\,du=\varphi(0)=\psi(0)=\Gamma(a)\Gamma(1-a)=\frac{\pi}{\sin\pi a}$$

Folgerung 2. Für $-1<s<1\,,\ n>0$ ist

$$\int_0^{\infty}x^{s-1}\frac{x}{4\pi^2n^2+x^2}\,dx=(2\pi)^{s-1}\frac{\pi}{2\cos\frac{\pi s}{2}}\,n^{s-1}$$

Beweis. Man setze in Folgerung 1

$$a=\frac{s+1}{2}\,,\quad u=\frac{x^2}{4\pi^2u^2}\,.$$

7.12 Beweis eines allgemeinen Satzes über verschränkte Produkte. (Mai 1932)

Hasse studies the inflation map for the second cohomology and its interpretation in terms of central simple algebras.

VII, 33

Verallgemeinerung eigener Untersuchung nach Anre– gungen von Artin und E. Noether.

Mai 1932.

Es sei Z/Ω galoissch, $\mathfrak{G}$ die Gruppe, ferner Z_0 ein galoisscher Teilkörper von Z/Ω, $\mathfrak{A}$ seine Invariantengruppe, und

$$r = [Z : Z_0] \,, \qquad (\text{Ordnung von } \mathfrak{A})\,.$$

Aus jedem Faktorensystem $(a^0) = \left(a^0_{\mathfrak{A}\mathsf{S},\mathfrak{A}\mathsf{T}}\right)$ von Z_0, bezogen auf die Darstellung der Gruppe von Z_0/Ω als Faktorgruppe $\mathfrak{G}/\mathfrak{A}$, kann man eindeutig ein Faktorensystem $(a) = (a_{\mathsf{S},\mathsf{T}})$ von Z herleiten durch die Festsetzung

$$a_{\mathsf{S},\mathsf{T}} = a^0_{\mathfrak{A}\mathsf{S},\mathfrak{A}\mathsf{T}}\,.$$

Dabei gilt dann:

Satz. *Es ist*

$$\begin{array}{lccc} & (Z,\, a) & \sim & (Z_0,\, a^0)\,, \\ \textit{genauer} & (Z,\, a) & = & (Z_0,\, a^0)_r\,. \end{array}$$

Beweis. $\mathfrak{B}$ sei eine Z_0–Basis von Z,

$$z\mathfrak{B} = \mathfrak{B}M_z$$

VII, 34 die durch sie vermittelte Matrizendarstellung r–ten Grades von Z in Z_0. Ferner sei

$$\mathfrak{B}^{\mathsf{S}} = \mathfrak{B}\mathsf{P}_{\mathsf{S}}$$

die durch sie vermittelte Darstellung von $\mathfrak{G}$ in Z_0. Sind dann $u^0_{\mathfrak{A}\mathsf{S}}$ die den $\mathfrak{A}\mathsf{S}$ aus $\mathfrak{G}/\mathfrak{A}$ zugeordneten Operatoren in $(Z_0,\, a^0)$, so setze ich

$$u_{\mathsf{S}} = u^0_{\mathfrak{A}\mathsf{S}}\mathsf{P}_{\mathsf{S}}^{-1}\,;$$

das sind Matrizen vom Grade r mit Koeffizienten aus $(Z_0,\, a^0)$. Ich zeige, daß sie als Operatoren für die S mit den M_z als Darstellung von Z zusammen gerade $(Z,\, a)$ mit dem oben definierten Faktorensystem (a) erzeugen.

In der Tat ist einerseits

$$z^{\mathsf{S}}\mathfrak{B}^{\mathsf{S}} = \mathfrak{B}^{\mathsf{S}} M_z^{\mathfrak{A}\mathsf{S}}$$

also

$$\begin{aligned} z^{\mathsf{S}}\mathfrak{B}\mathsf{P}_{\mathsf{S}} &= \mathfrak{B}\mathsf{P}_{\mathsf{S}} M_z^{\mathfrak{A}\mathsf{S}} \\ &= \mathfrak{B}\mathsf{P}_{\mathsf{S}} u_{\mathsf{S}}^{0\;-1} M_z u_{\mathsf{S}}^0 \end{aligned}$$

also schließlich

$$\begin{aligned} z^{\mathsf{S}}\mathfrak{B} &= \mathfrak{B}\mathsf{P}_{\mathsf{S}} u_{\mathsf{S}}^{0\;-1} M_z u_{\mathsf{S}}^0 \mathsf{P}_{\mathsf{S}}^{-1} \\ &= \mathfrak{B} u_{\mathsf{S}}^{-1} M_z u_{\mathsf{S}}\,, \end{aligned}$$

und somit

$$M_{z^{\mathsf{S}}} = u_{\mathsf{S}}^{-1} M_z u_{\mathsf{S}}\,;$$

andrerseits

VII, 35

$$\begin{aligned} u_{\mathsf{S}} u_{\mathsf{T}} &= u_{\mathfrak{A}\mathsf{S}}^0 \mathsf{P}_{\mathsf{S}}^{-1} u_{\mathfrak{A}\mathsf{T}}^0 \mathsf{P}_{\mathsf{T}}^{-1} \\ &= u_{\mathfrak{A}\mathsf{S}}^0 u_{\mathfrak{A}\mathsf{T}}^0 \mathsf{P}_{\mathsf{S}}^{-\mathsf{T}} \mathsf{P}_{\mathsf{T}}^{-1} \\ &= u_{\mathfrak{A}\mathsf{S}\mathsf{T}}^0 a_{\mathfrak{A}\mathsf{S},\mathfrak{A}\mathsf{T}}^0 \mathsf{P}_{\mathsf{S}}^{-\mathsf{T}} \mathsf{P}_{\mathsf{T}}^{-1} \\ &= u_{\mathsf{S}\mathsf{T}} a_{\mathsf{S},\mathsf{T}} \mathsf{P}_{\mathsf{S}\mathsf{T}} \mathsf{P}_{\mathsf{S}}^{-\mathsf{T}} \mathsf{P}_{\mathsf{T}}^{-1}\,, \end{aligned}$$

während aus

$$\mathfrak{B}^{\mathsf{S}\mathsf{T}} = \mathfrak{B}^{\mathsf{T}} \mathsf{P}_{\mathsf{S}}^{\mathsf{T}} = \mathfrak{B}\mathsf{P}_{\mathsf{T}} \mathsf{P}_{\mathsf{S}}^{\mathsf{T}}$$

folgt

$$\mathsf{P}_{\mathsf{S}\mathsf{T}} = \mathsf{P}_{\mathsf{T}} \mathsf{P}_{\mathsf{S}}^{\mathsf{T}}\,,$$

sodaß also in der Tat

$$u_{\mathsf{S}} u_{\mathsf{T}} = u_{\mathsf{S}\mathsf{T}}\, a_{\mathsf{S},\mathsf{T}}$$

ist.

Hiernach sind die Relationen von $(Z,\, a)$ innerhalb $(Z_0,\, a^0)_r$ erfüllt, d. h. es liegt eine homomorphe Abbildung von $(Z,\, a)$ auf ein Teilsystem von $(Z_0,\, a^0)_r$

vor. Da $(Z,\, a)$ einfach ist, muß die Abbildung isomorph sein (das Nullsystem kommt nicht in Frage), und aus Gradgründen ist dann in der Tat

$$(Z,\, a) = (Z_0,\, a^0)_r\,.$$

VII, 36 **Zyklischer Spezialfall.**

Ist Z/Ω zyklisch so sind die Faktorensysteme (a^0), (a) durch Zahlen α_0, α aus Ω gegeben, und zwar ist, wenn $\mathfrak{G}$ durch S erzeugt wird und die Operatoren von $(Z_0,\, a^0) = (a_0,\, Z,\, \mathsf{S})$ in der üblichen Weise als die Potenzen eines einzigen $u^0_{\mathfrak{A}\mathsf{S}}$ mit ${u^0_{\mathfrak{A}\mathsf{S}}}^{n_0} = \alpha_0 \quad \big(n_0 = \text{Grad von } Z_0\big)$ normiert sind,

$$u_{\mathsf{S}}^{n_0} = \big(u^0_{\mathfrak{A}\mathsf{S}} \mathsf{P}_{\mathsf{S}}^{-1}\big)^{n_0} = \alpha_0\, \mathsf{P}_{\mathsf{S}}^{-(\mathsf{S}^{n_0-1} + \cdots + \mathsf{S} + 1)},$$

also, wegen $\mathsf{P}_{\mathsf{S}}^{\mathsf{S}^{n_0}} = \mathsf{P}_{\mathsf{S}}$, weiter für den Grad $n = n_0 r$ von Z als Exponenten:

$$u_{\mathsf{S}}^{n} = \alpha_0^r\, \mathsf{P}_{\mathsf{S}}^{-(\mathsf{S}^{n-1} + \cdots + \mathsf{S} + 1)},$$

während doch wegen $\mathfrak{B} = \mathfrak{B}^{\mathsf{S}^n} = \mathfrak{B}\mathsf{P}_{\mathsf{S}}^{1+\mathsf{S}+\cdots+\mathsf{S}^{n-1}}$ der letzte Faktor 1 ist, also

$$u_{\mathsf{S}}^{n} = \alpha_0^r, \quad \text{d. h. } \ \alpha = \alpha_0^r$$

Damit folgt also die Identität:

$$\boldsymbol{(\alpha_0^r,\, Z,\, \mathsf{S}) = (\alpha_0,\, Z_0,\, \mathfrak{A}\mathsf{S})_r}\,.$$

7.13 Haupthilfssatz zum völlig reellen Beweis der Riemannschen Funktionalgleichung. (Mai 1932)

A lemma for a "real" proof of the functional equation of Riemann's zeta function, following Landau. See also 7.11.]

VII, 37

Nach Landau, Mai 1932

Es kommt auf den reellen Beweis der Formel

$$(1) \qquad \int_0^\infty x^{s-1} \begin{matrix}\cos\\ \sin\end{matrix}\, x\,dx = \Gamma(s) \begin{matrix}\cos\\ \sin\end{matrix}\, \frac{\pi s}{2} \qquad \text{für } 0 < s < 1$$

an.

Hilfssatz 1. Es seien $s > 0$ und $\delta > 0$ fest, ferner

$$\left.\begin{aligned} \varphi(y) &= \int_0^\infty x^{s-1}\, e^{-(\delta+iy)x} dx \\ \psi(y) &= \frac{\Gamma(s)}{(\delta^2+y^2)^{\frac{s}{2}}}\, e^{-si \operatorname{arctg} \frac{y}{\delta}} \end{aligned}\right\} \quad \text{für beliebiges reelles } y\,.$$

Dann ist

$$\varphi(y) = \psi(y)\,,$$

also insbesondere $(y = 1)$:

$$(2) \qquad \int_0^\infty x^{s-1}\, e^{-(\delta+i)x} dx = \frac{\Gamma(s)}{(\delta^2+1)^{\frac{s}{2}}}\, e^{-(si \operatorname{arctg} \frac{1}{\delta})}.$$

Beweis. $\int_0^\infty x^s\, e^{-(\delta+yi)x} dx$ konvergiert gleichmäßig in y. Also

VII, 38

$$\begin{aligned}\varphi'(y) &= -i\int_0^\infty x^s\, e^{-(\delta+yi)x}dx \\ &= ix^s\,\frac{e^{-(\delta+yi)x}}{\delta+yi}\bigg|_0^\infty - \frac{si}{\delta+yi}\int_0^\infty x^{s-1}\, e^{-(\delta+yi)x}dx \\ &= \frac{-si}{\delta+yi}\,\varphi(y)\end{aligned}$$

Ferner ist

$$\begin{aligned}\psi'(y) &= \Gamma(s)\, e^{-si\operatorname{arctg}\frac{y}{\delta}}\left(\frac{-sy}{(\delta^2+y^2)^{\frac{s}{2}+1}} - \frac{1}{(\delta^2+y^2)^{\frac{s}{2}}}\,\frac{si\delta}{\delta^2+y^2}\right) \\ &= -si\,\Gamma(s)e^{-si\operatorname{arctg}\frac{y}{\delta}}\,\frac{\delta-yi}{(\delta^2+y^2)^{\frac{s}{2}+1}} \\ &= \frac{-si}{\delta+yi}\,\psi(y)\,.\end{aligned}$$

Zusammengenommen:

$$\left(\frac{\varphi}{\psi}\right)' = \frac{\psi\varphi'-\varphi\psi'}{\psi^2} = 0$$
$$\varphi(y) = c\cdot\psi(y)\,,\quad c = c(s,\,\delta)$$

Nun ist

$$\begin{aligned}\varphi(0) &= \int_0^\infty x^{s-1}\, e^{-\delta x}dx = \frac{1}{\delta^s}\,\Gamma(s) \\ \psi(0) &= \frac{1}{\delta^s}\,\Gamma(s)\,,\end{aligned}$$

VII, 39 also $c=1$, was die Behauptung ergibt. *Hilfssatz 2.* $\int_0^\infty x^{s-1}\, e^{-(\delta+i)x}dx$ konvergiert bei festem s mit $0<s<1$ für $\delta \geqq 0$ gleichmäßig.

Beweis. a.) Bei $x=0$ ist dies klar.
b.) Für $\delta \geqq 0\,,\ 0<a<b$ ist nach dem 2. Mittelwertsatz

$$\left|\int_a^b x^{s-1}\, e^{-\delta x}\,\begin{matrix}\cos\\ \sin\end{matrix}\ x\,dx\right| = a^{s-1}\, e^{-\delta a}\left|\int_a^\xi \begin{matrix}\cos\\ \sin\end{matrix}\ x\,dx\right|,$$

wo der Mittelwert $\xi = \xi(\delta, s, a, b)$ im Intervall $a \leqq \xi \leqq b$ liegt, also

$$\left| \int_a^b x^{s-1} e^{-\delta x} \begin{matrix} \cos \\ \sin \end{matrix} x \, dx \right| \leqq 2a^{s-1},$$

unabhängig von b.

Nunmehr folgt der Beweis von (1) ohne weiteres, indem man gemäß Hilfssatz 2 im Ergebnis (2) von Hilfssatz 1 $\delta \to 0$ gehen läßt.

7.14 Ansätze zum elementaren Beweis des Satzes von der arithmetischen Progression. (Mai 1932)

Ideas for elementary proofs of Dirichlet's Theorem on primes in arithmetic progression. Here Hasse shows that there are infinitely many primes $q \equiv 1 \bmod p$.

VII, 40

Mai 1932

Ich knüpfe an den Beweis von Satz 1 auf S. 29] an. Das dortige a wähle ich jetzt folgenden beiden Bedingungen genügend:

$$\begin{array}{lrcl} 1.) & a & \not\equiv & 1 \text{ mod. } p \\ 2.) & a^{p-1} & \not\equiv & 1 \text{ mod. } p^2. \end{array}$$

Dann wird wegen 1.) nach dem früher Gezeigten

$$f_\nu(a) \equiv 1 \text{ mod. } p^\nu. \tag{1}$$

Denn $f_\nu(a)$ wird prim zu p, und jeder seiner Primteiler q wird $\equiv 1$ mod. p^ν. Wegen 2.) wird ferner

$$f_\nu(a) \not\equiv 1 \text{ mod. } p^{\nu+1}. \tag{2}$$

Denn sonst folgte

$$a^{p^\nu} \equiv a^{p^{\nu+1}} \text{ mod. } p^{\nu+1},$$

d. h.

$$a^{p^{\nu-1}(p-1)} \equiv 1 \text{ mod. } p^{\nu+1},$$

und somit

$$a^{p-1} \equiv 1 \text{ mod. } p^2.$$

VII, 41

p ist dabei als *ungerade* Primzahl vorausgesetzt.

Aus (1) und (2) folgt ein rein arithmetischer Beweis des Satzes:

Ist p ungerade Primzahl, so gibt es für jedes $\nu \geqq 1$ Primzahlen q_ν mit

$$q_\nu \equiv 1 \text{ mod. } p^\nu, \; q_\nu \not\equiv 1 \text{ mod. } p^{\nu+1}.$$

Insbesondere gibt es also für jedes ν unendlich viele Primzahlen q mit

$$q \equiv 1 \text{ mod. } p^\nu.$$

7.15 Hyperkomplexer Beweis eines Satzes aus der Chevalleyschen Thèse. (Mai 1932)

Chevalley's thesis [Che33b] *appeared in print in 1933 only but Hasse had got a preprint. This entry gives a proof, using the theory of algebras, of a certain result in cohomology which is used to transfer local class field theory from the cyclic to the general abelian case. (In this process, also the result of the next entry] is used.) Chevalley too wrote a separate paper, independent of his thesis, containing this.* [Che33a].

VII, 42

Mai 1932

Satz. *Seien K, K' unabhängige zyklische Körper erster Art vom Grade n über k und K'' ein zyklischer Teilkörper ihres Kompositums KK', der von K und K' unabhängig ist.*

Ist dann ein Element α aus k Norm sowohl aus K als auch aus K', so ist α auch Norm aus K''.

Beweis. Seien S, S' Erzeugende der Gruppen von K, K' und so, daß K' bei S, K bei S' elementweise invariant bleibt. Die Gruppe von KK' ist dann das direkte Produkt der beiden durch S und S' erzeugten Zyklen.

K'' gehört zu einer derartigen Untergruppe mit zyklischer Faktorgruppe, daß die Komposition sowohl mit S als auch mit S' die ganze Gruppe ergibt. Eine solche Untergruppe ist durch eine lineare Kongruenz $ax + a'x' \equiv 0 \mod n$ für die Exponenten der Basisdarstellung $\mathsf{S}^x \mathsf{S}'^{x'}$ definiert, bei der jeder gemeinsame Teiler von a und n auch in a' aufgeht, und ebenso jeder gemeinsame Teiler von a' und n auch in a aufgeht: VII, 43

$$(a, n) = (a', n) = (a, a', n)\,.$$

Denn sonst gäbe es nicht Lösungen mit zu n primem x, bzw. mit zu n primem x'. Eine solche Kongruenz kann also nach Wegdivision des Teilers in der Form

$$a_0 x + a_0' x' \equiv 0 \mod n_0$$

geschrieben werden, wo

$$(a_0, n) = (a_0', n) = 1$$

ist, und besitzt die Lösung

$$x = a_0' \,, \quad x' = -a_0$$

VII, 44 in der x und x' *gleichzeitig* prim zu n sind. Somit enthält (bei geeigneter Normierung) die fragliche Untergruppe das Produkt $\mathsf{SS'}$. Es genügt dann, die Behauptung für den vollen Invariantenkörper K'' von $\mathsf{SS'}$ zu beweisen, da sie dann für Teilkörper a fortiori richtig ist. Soweit die Chevalleysche Vorbereitung.

Nunmehr sei A das zu KK' gehörige verschränkte Produkt mit dem aus

$$u^n = \alpha \,, \quad {u'}^n = \alpha^{-1}, \quad u'u = uu'$$

bestimmten Faktorensystem ($u \leftrightarrow \mathsf{S}\,,\ u' \leftrightarrow \mathsf{S'}$). Wegen der elementweisen Vertauschbarkeit von u mit K', u' mit K, ist ersichtlich

$$A = (\alpha,\, K,\, \mathsf{S}) \times (\alpha^{-1},\, K',\, \mathsf{S'})$$

Da hier nach Voraussetzung über α beide direkten Faktoren ~ 1 sind, ist $A \sim 1$.

Nun besitzt aber A auch noch eine andere direkte Zerlegung. Führt man VII, 45 nämlich u, uu' als Operatoren statt u, u' ein, so gehen die Relationen über in

$$u^n = \alpha \,,\ (uu')^n = 1 \,,\ (uu')u = u(uu') \,.$$

Da u mit K', uu' mit K'' elementweise vertauschbar ist, und KK' auch als $K'K''$ geschrieben werden kann, erhält man

$$\begin{aligned} A &= (\alpha,\, K'',\, \mathsf{S}) \times (1,\, K',\, \mathsf{SS'}) \\ &\sim (\alpha,\, K'',\, \mathsf{S}) \,. \end{aligned}$$

Wegen $A \sim 1$ folgt in der Tat, daß α Norm auch aus K'' ist.

Bemerkung. Genau so folgt allgemeiner: Ist für $\mathfrak{p}$–adische K, K'

$$\left(\frac{\alpha,\, K}{\mathfrak{p}}\right) = \mathsf{S} \qquad \left(\frac{\alpha,\, K'}{\mathfrak{p}}\right) = \mathsf{S'},$$

so ist

$$\left(\frac{\alpha,\, K''}{\mathfrak{p}}\right) = 1 \,,$$

wenn K'' der zu $\mathsf{SS'}$ gehörige Invariantenkörper in KK' ist.

7.16 Ein Satz über verschränkte Produkte. (Mai 1932)

A theorem on crossed products. See the foregoing entry.]. See also 7.23.]

VII, 46

Mai 1932

Es sei K/k galoissch, Gruppe $\mathfrak{G} = \mathfrak{Z} \times \mathfrak{H}$, wo $\mathfrak{Z} = \{\mathsf{S}\}$ zyklisch, Ordnung n. Ferner

Z	der	Invariantenkörper	zu	$\mathfrak{H}$,	also	Z/k	zyklisch,	Grad n,
L	"	"	"	$\mathfrak{Z}$,	"	K/L	"	"

Das allgemeine verschränkte Produkt A zu K ist durch Relationen folgender Form definiert:

$$xu = ux^{\mathsf{S}}, \qquad xu_{\mathsf{T}} = u_{\mathsf{T}}x^{\mathsf{T}}$$
$$u^n = a\,, \qquad u_{\mathsf{T}}u = uu_{\mathsf{T}}b_{\mathsf{T}}\,, \qquad u_{\mathsf{T}}u_{\mathsf{T}'} = u_{\mathsf{T}\mathsf{T}'}c_{\mathsf{T},\mathsf{T}'}\,.$$

Dabei bezeichnen x, bzw. T, T' variable Elemente aus K, bzw. $\mathfrak{H}$, ferner a, b_{T}, $c_{\mathsf{T},\mathsf{T}'}$ feste Elemente aus K (das Faktorensystem) mit den (Schreierschen) Relationen (außer den Assoziativformeln für die c allein):

$$a^{1-\mathsf{S}} = 1\,, \quad b_{\mathsf{T}}^{N} = a^{1-\mathsf{T}}, \quad c_{\mathsf{T},\mathsf{T}'}^{\mathsf{S}-1} = \frac{b_{\mathsf{T}}^{\mathsf{T}'}b_{\mathsf{T}'}}{b_{\mathsf{T}\mathsf{T}'}}\,,$$

wo zur Abkürzung $N = 1 + \mathsf{S} + \cdots + \mathsf{S}^{n-1}$ gesetzt ist.

VII, 47

Ich schreibe kurz:

$$A = (a,\, b_{\mathsf{T}},\, c_{\mathsf{T},\mathsf{T}'},\, K)\,.$$

Satz. *Es ist*

$$A^n \sim (c_{\mathsf{T},\mathsf{T}'}^{N},\, L)\,.$$

Beweis. Jedenfalls ist

$$A^n \sim (a^n,\, b_{\mathsf{T}}^n,\, c_{\mathsf{T},\mathsf{T}'}^n,\, K)\,.$$

Sei ausführlich entsprechend:

$$xU = Ux^{\mathsf{S}}, \qquad xU_{\mathsf{T}} = U_{\mathsf{T}}x^{\mathsf{T}}$$
$$U^n = a^n, \qquad U_{\mathsf{T}}U = UU_{\mathsf{T}}b_{\mathsf{T}'}^n \qquad U_{\mathsf{T}}U_{\mathsf{T}'} = U_{\mathsf{T}\mathsf{T}'}c_{\mathsf{T},\mathsf{T}'}^n\,.$$

Dann setze ich

$$U = va\,, \quad U_{\mathsf{T}} = v_{\mathsf{T}} b_{\mathsf{T}}^{\frac{N-n}{1-\mathsf{S}}}\,.$$

Nach den Schreierschen Relationen wird:

$$xv = vx^{\mathsf{S}}, \qquad xv_{\mathsf{T}} = v_{\mathsf{T}} x^{\mathsf{T}}$$
$$v^n = 1\,, \qquad v_{\mathsf{T}} v = v v_{\mathsf{T}}\,, \qquad v_{\mathsf{T}} v_{\mathsf{T}'} = v_{\mathsf{T}\mathsf{T}'} c_{\mathsf{T},\mathsf{T}'}^N\,.$$

Hiernach zerfällt A^n direkt:

$$A^n \sim (a^n,\, b_{\mathsf{T}}^n,\, c_{\mathsf{T},\mathsf{T}'}^n,\, K) = (1,\, Z,\, \mathsf{S}) \times (c_{\mathsf{T},\mathsf{T}'}^N,\, L) \sim (c_{\mathsf{T},\mathsf{T}'}^N,\, L)\,.$$

VII, 48

Der Satz läßt sich auch auf den Fall verallgemeinern, wo $\mathfrak{Z}$ nicht mehr zyklisch, sondern *irgendeine* Gruppe der Ordnung n ist. Das allgemeine verschränkte Produkt A zu K ist dann durch Relationen folgender Form definiert:

$$xu_{\mathsf{S}} = u_{\mathsf{S}} x^{\mathsf{S}} \qquad xu_{\mathsf{T}} = u_{\mathsf{T}} x^{\mathsf{T}}$$
$$u_{\mathsf{S}} u_{\mathsf{S}'} = u_{\mathsf{S}\mathsf{S}'} a_{\mathsf{S},\mathsf{S}'} \qquad u_{\mathsf{T}} u_{\mathsf{S}} = u_{\mathsf{S}} u_{\mathsf{T}} b_{\mathsf{S},\mathsf{T}} \qquad u_{\mathsf{T}} u_{\mathsf{T}'} = u_{\mathsf{T}\mathsf{T}'} c_{\mathsf{T},\mathsf{T}'}$$

Dabei bezeichnen x; S, S'; T, T' bzw. variable Elemente aus K, $\mathfrak{Z}$, $\mathfrak{H}$, ferner die a, b, c feste Elemente aus K (das Faktorensystem) mit den Relationen (außer den Assoziativformeln für die a allein und c allein)

$$b_{\mathsf{S},\mathsf{T}}^{N_{\mathsf{S}}} = a_{\mathsf{S},\mathsf{S}'}^{1-\mathsf{T}} \qquad b_{\mathsf{S},\mathsf{T}}^{N_{\mathsf{T}}} = c_{\mathsf{T},\mathsf{T}'}^{\mathsf{S}-1}.$$

Dabei ist zur Abkürzung für jede mit den S indizierte Zahlfolge α_{S} gesetzt:

$$\alpha_{\mathsf{S}}^{N_{\mathsf{S}}} = \frac{\alpha_{\mathsf{S}}^{\mathsf{S}'}\, \alpha_{\mathsf{S}'}}{\alpha_{\mathsf{S}\mathsf{S}'}}$$

und entsprechend für die T.

Ich schreibe kurz:

$$A = (a_{\mathsf{S},\mathsf{S}'},\; b_{\mathsf{S},\mathsf{T}},\; c_{\mathsf{T},\mathsf{T}'} \mid K)\,.$$

VII, 49

NB. Siehe den vereinfachten Beweis von Witt, S. 96] f.

Satz. *Es ist*

$$A^n \sim \left(c_{\mathsf{T},\mathsf{T}'}^{\Sigma},\, L\right),$$

wo $\sum$ *die Summe aller* S *bezeichnet, also* $c^{\sum}_{\mathsf{T},\mathsf{T}'}$ *die Normen bezgl.* L *von den* $c_{\mathsf{T},\mathsf{T}'}$ *sind.*

Beweis. Zunächst ist wieder

$$A^n \sim (a^n_{\mathsf{S},\mathsf{S}'},\, b^n_{\mathsf{S},\mathsf{T}},\, c^n_{\mathsf{T},\mathsf{T}'} \mid K)\,.$$

Seien U die diesem verschränkten Produkt entsprechenden Transformatoren. Dann setze ich:

$$U_{\mathsf{S}} = v_{\mathsf{S}} \prod_{\mathsf{R}} a_{\mathsf{R},\mathsf{S}} \qquad V_{\mathsf{T}} = v_{\mathsf{T}} \left(\prod_{\mathsf{R}} b_{\mathsf{R},\mathsf{T}}\right)^{-1}.$$

Dann wird, durch Übergang zu den Transformatoren v,

$$A^n \sim \Big(a^n_{\mathsf{S},\mathsf{S}'} \big(\prod_{\mathsf{R}} a_{\mathsf{R},\mathsf{S}}\big)^{-N_{\mathsf{S}}},\; b^n_{\mathsf{S},\mathsf{T}} \big(\prod_{\mathsf{R}} a_{\mathsf{R},\mathsf{S}}\big)^{\mathsf{T}-1} \big(\prod_{\mathsf{R}} b_{\mathsf{R},\mathsf{T}}\big)^{\mathsf{S}-1},$$
$$c^n_{\mathsf{T},\mathsf{T}'} \big(\prod_{\mathsf{R}} b_{\mathsf{R},\mathsf{T}}\big)^{N_{\mathsf{T}}} \mid K\Big)\,.$$

Nun ist nach den Assoziativrelationen für die a:

$$\left(\prod_{\mathsf{R}} a_{\mathsf{R},\mathsf{S}}\right)^{N_{\mathsf{S}}} = a^n_{\mathsf{S},\mathsf{S}'}\,.$$

Ferner ergibt sich unter Anwendung obiger Relationen:

$$\big(\prod_{\mathsf{R}} a_{\mathsf{R},\mathsf{S}}\big)^{\mathsf{T}-1} = \left(\prod_{\mathsf{R}} \frac{b^{\mathsf{S}}_{\mathsf{R},\mathsf{T}} b_{\mathsf{S},\mathsf{T}}}{b_{\mathsf{RS},\mathsf{T}}}\right)^{-1} = \big(\prod_{\mathsf{R}} b_{\mathsf{R},\mathsf{T}}\big)^{1-\mathsf{S}} \cdot b^{-n}_{\mathsf{S},\mathsf{T}}\,,$$
$$\big(\prod_{\mathsf{R}} b_{\mathsf{R},\mathsf{T}}\big)^{+N_{\mathsf{T}}} = \prod_{\mathsf{R}} b^{+N_{\mathsf{T}}}_{\mathsf{R},\mathsf{T}} = \prod_{\mathsf{R}} c^{\mathsf{R}-1}_{\mathsf{T},\mathsf{T}'} = c^{\sum}_{\mathsf{T},\mathsf{T}'} \cdot c^{-n}_{\mathsf{T},\mathsf{T}'}\,.$$

Zusammengenommen:

$$A^n \sim (1,\; 1,\; c^{\sum}_{\mathsf{T},\mathsf{T}'} \mid K) \quad \text{und daraus wie oben die Beh.}$$

7.17 Verschiedenes aus und zu Chevalley's Thèse. (Mai 1932)

Chevalley's thesis was the second great general presentation of class field theory after Hasse's report [Has26a]*, with essential simplifications and new ideas. These were largely based on the work of Artin and Hasse, as well as of Herbrand and Chevalley himself. In the present entry Hasse notes the basic steps of Chevalley's setup. The thesis appeared in print in the year 1933 only* [Che33b]*; obviously Hasse used here his mimeographed copy.*

VII, 50

Mai 1932

I. *Wenn K/k zyklisch vom Grade n und k die n–te Einheitswurzel ζ enthält, ist $K = k(\sqrt[n]{\alpha})$.*

Kurzer Beweis. Es ist $\zeta^n = N_{Kk}(\zeta) = 1$. Nach „Zahlbericht, Satz 90" ist also $\zeta = \mathsf{A}^{\mathsf{S}-1}$, wo A Zahl aus K und S erzeugenden Automorphismus von K/k bedeutet. Hierbei sind $\mathsf{A}, \mathsf{A}^{\mathsf{S}}, \ldots, \mathsf{A}^{\mathsf{S}^{n-1}}$ verschieden, d. h. $K = k(\mathsf{A})$. Und es ist $\mathsf{A}^{n\mathsf{S}} = \mathsf{A}^n$, d. h. $\mathsf{A}^n = \alpha$ in k.

II. *Zweckmäßiges Arrangement der Theorie der Kummerschen Körper.*

1.) $\left[k(\sqrt[n]{\alpha_0}) : k\right] = [\alpha_0\alpha^n : \alpha^n]$.

2.) Wenn B in $k(\sqrt[n]{\alpha_0})$ und B^n in k, dann $\mathsf{B} = \sqrt[n]{\alpha_0}^{\,x}\beta$ mit β aus k.

3.) *Hauptsatz*: Ist γ eine die α^n enthaltende Zahlgruppe in k, so ist $\left[k(\sqrt[n]{\gamma}) : k\right] = [\gamma : \alpha^n]$. (Dabei bezeichnet $k(\sqrt[n]{\gamma})$ den durch Adjunktion *aller* $\sqrt[n]{\gamma}$ zu k entstehenden Körper.)

VII, 51 *Beweis.* Durch vollständige Induktion.

III. *Ist $k_{\mathfrak{p}}$ eine $\mathfrak{p}$–adische Erweiterung von k, K eine Erweiterung endlichen Grades von k, $K_{\mathfrak{P}}$ eine zugehörige $\mathfrak{P}$–adische Erweiterung, und ist $\alpha \equiv N(\mathsf{A}_n)$* mod $\mathfrak{p}^n$ *mit A_n aus K für jedes n, so ist $\alpha = N_{\mathfrak{p}}(\mathsf{A}_{\mathfrak{P}})$ mit $\mathsf{A}_{\mathfrak{P}}$ aus $K_{\mathfrak{P}}$, wo $N_{\mathfrak{p}}$ die Norm bzgl. $k_{\mathfrak{p}}$ bedeutet.*

Kurzer Beweis. Sei $\mathsf{A}_n^0 \equiv \mathsf{A}_n \mod \mathfrak{P}^{en}$, $\equiv 1$ mod. $\frac{\mathfrak{p}^n}{\mathfrak{P}^{en}}$ (e Ordnung von $\mathfrak{P}$ bzgl. $\mathfrak{p}$), so ist A_n^0 eine beschränkte unendliche Menge in $K_{\mathfrak{P}}$. Wegen der Kompaktheit

von $K_{\mathfrak{P}}$ besitzt sie Häufungsstelle $\mathsf{A}_{\mathfrak{P}}$ in $K_{\mathfrak{P}}$, also eine gegen $\mathsf{A}_{\mathfrak{P}}$ konvergente Teilfolge $\mathsf{A}^0_{n_\nu}$:

$$\lim_{\nu\to\infty} \mathsf{A}^0_{n_\nu} = \mathsf{A}_{\mathfrak{P}}\,, \quad \text{d.h.} \quad \mathsf{A}^0_{n_\nu} \equiv \mathsf{A}_{\mathfrak{P}} \mod \mathfrak{P}^{r_\nu} \qquad \begin{array}{l}\text{mit } n_\nu \to \infty \\ \text{und } r_\nu \to \infty \\ \text{für } \nu \to \infty\end{array}$$

Dann folgt

$$N_{\mathfrak{p}}(\mathsf{A}_{\mathfrak{P}}) \equiv N_{\mathfrak{p}}(\mathsf{A}^0_{n_\nu}) \text{ mod. } \mathfrak{P}^{r_\nu}, \quad \text{dh. mod. } \mathfrak{p}^{\left\{\frac{r_\nu}{e}\right\}}.$$

Ferner ist

$$N_{\mathfrak{p}}(\mathsf{A}^0_{n_\nu}) \equiv N(\mathsf{A}_{n_\nu}) \equiv \alpha \text{ mod. } \mathfrak{p}^{n_\nu}.$$

Also

$$N_{\mathfrak{p}}(\mathsf{A}_{\mathfrak{P}}) \equiv \alpha \mod \mathfrak{p}^{\,\mathrm{Min}\left(n_\nu,\, \left\{\frac{r_\nu}{e}\right\}\right)}.$$

Da auch der Exponent von $\mathfrak{p}$ mit $\nu \to \infty$ gegen ∞ geht, folgt die Behauptung.

IV. *Ist* K/k *abelsch, so nimmt das Artin–Symbol* $\left(\frac{K}{\mathfrak{a}}\right)$ *jeden Wert der Gruppe von* K/k *für ein geeignetes* $\mathfrak{a}$ *an.* VII, 52

Beweis. Durch Betrachtung von K über geeigneten Teilkörpern reduziert sich die Behauptung zunächst auf den folgenden Satz:

> Ist K/k zyklisch vom Primzahlpotenzgrad p^ν, so gibt es ein in K unzerlegtes Primideal aus k.

Gäbe es nun kein solches, so wären in dem Teilkörper K_1 vom Grade p alle Primideale aus k zerlegt, also dessen Takagi–Gruppe (nach beliebigem mod. $\mathfrak{m}$) vom Index 1. Nach der „fundamentalen Ungleichungsfolge" (rein arithmetisch begründet.") ist das unmöglich, weil diese $h \geqq p$ ergibt. —

NB. Es folgt überdies sogar die Existenz eines *zu* $\mathfrak{m}$ *primen* unzerlegten Primideals im Spezialfall, also die Existenz eines *zu* $\mathfrak{m}$ *primen* $\mathfrak{a}$ mit $\left(\frac{K}{\mathfrak{a}}\right)$ gegeben im allgemeinen Fall, und damit insbesondere die Existenz *unendlich vieler* solcher $\mathfrak{a}$.

V. *Aus* IV. *folgt sofort der Anordnungssatz* (*speziell also der Eindeutigkeitssatz*) *für die Artin–Gruppen.* VII, 53

Beweis (des nichttrivialen Teils). Sei $H \leqq H'$ für die Artin–Gruppen zu K, K'. Zu KK' gehört nun $[H, H'] = H$ als Artin–Gruppe. Nach IV. ist also der Grad von KK' ebenfalls nur der Index von H wie der Grad von K. Das ergibt $KK' = K$, also $K' \leqq K$.

VI. *Für zyklisches* K/k *ist die Artin–Gruppe* H^* *in der Takagi–Gruppe* H *enthalten* (*beide nach beliebigem* mod. $\mathfrak{m}$ *erklärt*). *Rein arithmetischer Beweis, wenn für zykl. rel. Kreiskörper bekannt.*

Sei S erzeugender Automorphismus von K/k. Nach IV. existiert $\mathfrak{a}$ (prim zu $\mathfrak{m}$) mit $\left(\frac{K}{\mathfrak{a}}\right) = \mathsf{S}$, d. h. Erzeugende d. Klassen nach Artin–Gruppe H^*. Es wird zunächst gezeigt, daß $\mathfrak{a}$ auch Erzeugende der Klassen nach der Takagi Gruppe H ist. Dazu genügt es, beliebige (zu $\mathfrak{m}$ prime) *Primidealpotenzen* $\mathfrak{p}^a \sim \mathfrak{a}^x$ (H) zu erweisen, wenn $\mathfrak{p}^a \sim \mathfrak{a}^x$ (H^*) bekannt ist. Dazu *zwei* zyklische Hilfskreiskörper, fremd zu K und zu einander.

VII, 54

1.) K'/k von einem Grad, der Multiplum des Grades n von K/k ist. Dann sei $\mathfrak{a}$ von vornherein so gewählt, daß $\mathfrak{a}$ Norm eines Ideals $\mathfrak{A}'_0$ aus dem Invariantenkörper K'_0 von SS' in KK' und

$$\left(\frac{KK'}{\mathfrak{A}'_0}\right) = \mathsf{SS}'.$$

Das geht nach IV. natürlich auch.

2.) K''/k so, daß $\mathfrak{p}^a$ nach der Artin=Takagi–Gruppe H'' zu Klasse von durch n teilbarer Ordnung gehört.

Sei

$$\left(\frac{KK''}{\mathfrak{p}^a}\right) = \mathsf{S}^x\mathsf{S}''.$$

Dann werde $\mathfrak{B}^*_0$ im Invariantenkörper K^*_0 von $\mathsf{S}^x\mathsf{S}'^x\mathsf{S}''$ in $KK'K''$ so gewählt, daß

$$\left(\frac{KK'K''}{\mathfrak{B}^*_0}\right) = \mathsf{S}^x\mathsf{S}'^x\mathsf{S}''.$$

Das geht wieder nach IV. $\mathfrak{B}'_0$ und $\mathfrak{b}$ seien die Normen von $\mathfrak{B}^*_0$ nach K'_0 und k. ($K'_0 \leqq K^*_0$, weil $\{\mathsf{SS}', \mathsf{S}^x\} \geqq \{\mathsf{S}^x\mathsf{S}'^x\mathsf{S}''\}$.) Dann ist $\mathfrak{B}'_0 \sim {\mathfrak{A}'_0}^x$ nach der Artin–Takagi–Gruppe H'_0 für KK'/K'_0, also $\mathfrak{b} \sim \mathfrak{a}^x$ (H).

Andererseits ist $\mathfrak{p}^a$ Norm eines $\mathfrak{Q}''_0$ aus dem Invariantenkörper K''_0 zu $\mathsf{S}^x\mathsf{S}''$ zufolge der Eigenschaften des Artin–Symbols (folgt daraus, daß $\left(\frac{KK''}{\mathfrak{p}}\right)$ die Zerlegungsgruppe von $\mathfrak{p}$ für KK'' erzeugt, also den Grad der Primteiler von $\mathfrak{p}$ bestimmt). Man hat also

VII, 55

$$\left(\frac{KK''}{\mathfrak{Q}''_0}\right) = \mathsf{S}^x\mathsf{S}''.$$

Ist $\mathfrak{B}''_0$ Norm von $\mathfrak{B}^*_0$ in K''_0 (wie oben ist $K''_0 \leqq K^*_0$), so folgt wie oben $\mathfrak{B}''_0 \sim \mathfrak{Q}''_0$ (H''_0), also $\mathfrak{b} \sim \mathfrak{p}^a$ (H).

Zusammengenommen: $\mathfrak{p}^a \sim \mathfrak{a}^x\ (H)$, wie behauptet.

Ist nunmehr $\prod \mathfrak{p}^a \sim 1\ (H^*)$, so $\mathfrak{a}^{\sum x} \sim 1\ (H^*)$, $\sum x \equiv 0\ (n)$, $\mathfrak{a}^{\sum x}$ Norm aus K, also $\mathfrak{a}^{\sum x} \sim 1\ (H)$, $\prod \mathfrak{p}^a \sim 1\ (H)$.

VII. *Nimmt man den $\mathfrak{p}$–adischen Verschiebungssatz und den $\mathfrak{p}$–adischen Isomorphiesatz für den zyklischen Fall als hyperkomplex bewiesen an, so folgt genau wie in* V. *der $\mathfrak{p}$–adische Anordnungs– und speziell Eindeutigkeitssatz für den zyklischen Fall.*

VIII. *Berechnung des Index der $\mathfrak{p}$–hyperprimären Zahlen nach der Herbrandschen Methode.*

k enthalte die n–ten Einheitswurzeln ζ, $\mathfrak{p}$ sei ein (endliches) Primideal von k. Der Index h der $\mathfrak{p}$–hyperprimären Zahlen in der Gruppe aller Zahlen $\neq 0$ aus k kann auch dargestellt werden als: VII, 56

$$h = [\alpha : \alpha^n], \quad \text{wo } \alpha \text{ beliebig} \neq 0 \text{ aus } k_{\mathfrak{p}}.$$

Bezeichnet T_1 und T_2 die beiden zueinander inversen homomorphen Abbildungen:

$$T_1 = (\alpha \to \alpha^n), \quad T_2 = (\alpha \to 1)$$

der Gruppe α, so hat man für den Herbrandschen Quotienten:

$$\frac{[\alpha_2 : T_1\alpha]}{[\alpha_1 : T_2\alpha]} = \frac{[\alpha : \alpha^n]}{[\zeta : 1]} = \frac{h}{n}.$$

Nach dem Herbrandschen Satz wird also:

$$h = n\,\frac{[\beta_2 : T_1\beta]}{[\beta_1 : T_2\beta]} = n\,\frac{[\beta : \beta^n]}{[\beta_1 : 1]},$$

wo β irgendeine Untergruppe von α von endlichem Index ist (für die dann ja von selbst T_1 und T_2 zueinander inverse homomorphe Abbildungen sind). VII, 57

Wir wählen $\beta \equiv 1 \bmod. \mathfrak{p}^m$ in $k_{\mathfrak{p}}$ mit hinreichend großem m, nämlich so groß, daß

1.) β keine n–te Einheitswurzel $\zeta \neq 1$ enthält. — Dann wird $\beta_1 = 1$, also $[\beta_1 : 1] = 1$, und somit
$$h = n[\beta : \beta^n].$$

2.) β im Henselschen Sinne Exponentialeinheit ist.

Dann wird β durch Logarithmierung isomorph auf die Gruppe $\gamma_m \equiv 0$ mod.$^+$ $\mathfrak{p}^m$ in $k_\mathfrak{p}$ abgebildet, und dabei entspricht β^n genau $n\gamma_m$. Durch Division mit π^m wird weiter γ_m isomorph auf die Gruppe γ aller ganzen Zahlen aus $k_\mathfrak{p}$ abgebildet, und dabei entspricht $n\gamma_m$ genau $n\gamma$, oder auch $\pi^\nu\gamma$, wo $\mathfrak{p}^\nu$ der in n steckende Bestandteil von $\mathfrak{p}$ (π genau durch $\mathfrak{p}^1$ teilbar), d. h. $n\gamma_m$ entspricht genau die Gruppe $\gamma_0 \equiv 0$ mod. $\mathfrak{p}^\nu$. Somit

$$h = n[\gamma : \gamma_0] = n \cdot \mathfrak{N}\mathfrak{p}^\nu.$$

VII, 58

IX. *Reduktion des Existenzbeweises der Klassenkörpertheorie im Großen auf den Fall, daß der Grundkörper die nötigen Einheitswurzeln enthält.*

Sei k beliebiger Grundkörper, H Idealgruppe mod $\mathfrak{m}$ in k, n der kleinste Exponent, für den H alle n–ten Idealpotenzen (prim zu $\mathfrak{m}$) enthält, und ζ eine n–te Einheitswurzel.

$\overline{H}$ sei die Gruppe mod. $\mathfrak{m}$ in $k(\zeta)$, deren Normen nach k in H fallen. Zu $\overline{H}$ sei bereits $\overline{K}$ als Klassenkörper bekannt, außerdem natürlich auch schon der Isomorphiesatz bewiesen, wonach $\overline{K}/k(\zeta)$ abelsch, ferner auch der Eindeutigkeitssatz.

Ich zeige zunächst: *Dann ist* $\overline{K}/k$ *abelsch*. Sei in der Tat T ein Automorphismus von $k(\zeta)/k$. Dann ist zunächst $\overline{K}^T = \overline{K}$, weil $\overline{K}^T$ Klassenkörper zu $\overline{H}^T = \overline{H}$ ist, nach dem Eindeutigkeitssatz. Daher ist $\overline{K}/k$ galoissch. Ferner enthält $\overline{H}$ alle $\overline{\mathfrak{a}}^{1-T}$ $\big(\overline{\mathfrak{a}}$ prim zu $\mathfrak{m}$ in $k(\zeta)\big)$, weil deren Norm nach k ja 1 ist. Daher ist $\left(\frac{\overline{K}}{\overline{\mathfrak{a}}}\right) = \left(\frac{\overline{K}}{\overline{\mathfrak{a}}^T}\right) = T^{-1}\left(\frac{\overline{K}}{\overline{\mathfrak{a}}}\right)T$ für alle zu $\mathfrak{m}$ primen $\overline{\mathfrak{a}}$ aus $k(\zeta)$; denn weil $\overline{K}/k(\zeta)$ Klassenkörper ist, ist (etwa auf IV. und VI. gestützt) die Artin–Gruppe mit der Takagi–Gruppe identisch. Nach IV. ergibt sich jetzt, daß T mit *allen* Automorphismen von $\overline{K}/k(\zeta)$ vertauschbar ist. Da $k(\zeta)/k$ selbst abelsch ist, also die T untereinander vertauschbar sind, folgt in der Tat, daß die Gruppe von $\overline{K}/k$ abelsch ist, wie behauptet.

VII, 59

Nach dem Umkehrsatz ist nun weiter $\overline{K}/k$ Klassenkörper zu einer Gruppe $H' \leqq H$, und daraus folgt daß auch zu H ein Teilkörper von $\overline{K}$ als Klassenkörper gehört.

X. *Jedes verzweigte Primideal geht im Führer auf.*

Das zeigt man in 2 Schritten:

1.) falls K/k zyklisch von Primzahlgrad, ist es Norm aus K, und zerfällt also nach dem Zerlegungsgesetz voll.

2.) falls $K/_k$ beliebig, vollständige Induktion.

7.18 Beweis des Existenzsatzes (0.3) in meiner Annalenarbeit (E. Noether zum 50. Geb.). (8. Juni 1932.)

This is a generalization of the lemma which Artin had used in his proof of his reciprocity law. (For that see 7.10.]) When Hasse in March 1932 provided a proof of Artin's reciprocity law by means of the theory of algebras [Has33a] *he used this generalization of Artin's lemma, but its proof was sketched only. Here he produces the full proof. Later, van der Waerdenave an elementary proof; see 7.22.]*

VII, 60

8. Juni 1932.

Der **Satz** lautet:

Gegeben eine Anzahl Primzahlen $p_1, \dots, p_r$ und ihnen zugeordnet natürliche Zahlen $k_1, \dots, k_r$. Dann gibt es stets eine zyklische Kongruenzklasseneinteilung der rationalen Zahlen, bei der $p_1, \dots, p_r$ jeweils in Klassen von durch $k_1, \dots, k_r$ teilbarer Ordnung liegen und zudem -1 in einer Klasse der Ordnung 2.

Der *Beweis* wird so geführt:

Sei k das kleinste gemeinsame Multiplum der Zahlen $2k_i$, p_i und 8, und sei Ω der Körper der k–ten Einheitswurzeln. Zuvor einige Hilfssätze.

VII, 61 **Hilfssatz 1.** *Es sei $a \neq 0, \pm 1$ eine rationale Zahl und $m > 1$ eine natürliche Zahl. Für keinen Primteiler ℓ von m sei a die ℓ–te Potenz einer rationalen Zahl.*

Dann hat $\mathsf{P}(\sqrt[m]{a})$ den Grad m über dem rationalen Zahlkörper P, d. h. $x^m - a$ ist irreduzibel in P.

Beweis. Sei $m = \prod_i \ell_i^{\nu_i}$ die Primzerlegung von m. Dann ist $\mathsf{P}(\sqrt[m]{a})$ aus den $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ zusammengesetzt. Für jedes i enthält a mindestens eine Primzahl p_i mit einem zu ℓ_i primen Exponenten.*) Für dieses p_i ist dann $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ voll verzweigt, also vom Grade $\ell_i^{\nu_i}$. Daher ist der Grad von $\mathsf{P}(\sqrt[m]{a})$ teilbar durch $\ell_i^{\nu_i}$. Da dies für alle i gilt, ist er teilbar durch m, also gleich m.

Hilfssatz 2. *Ist — unter den Voraussetzungen von Hilfssatz 1 — $\mathsf{P}(\sqrt[m]{a})$ galoissch, so ist $m = 2$.*

VII, 62 **Beweis**. Da, wie bereits gesagt, $\mathsf{P}(\sqrt[m]{a})$ aus den $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ komponiert ist, kann

*) Stimmt nicht, da ev. auch -1 zu 2 primen Exponenten haben kann.

jeder Automorphismus von $\mathsf{P}(\sqrt[m]{a})$ durch ein System von Isomorphismen der $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ beschrieben werden. Solcher Systeme gibt es genau m. Da $\mathsf{P}(\sqrt[m]{a})$ den Grad m hat, kommen also *alle* diese Systeme als Automorphismen von $\mathsf{P}(\sqrt[m]{a})$ vor, und bilden die Gruppe von $\mathsf{P}(\sqrt[m]{a})$.

Betrachten wir jetzt einen Teilkörper $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$. Er ist vom Grade $\ell_i^{\nu_i}$, also $\mathsf{P}(\sqrt[m]{a})$ über ihn vom Grade $\dfrac{m}{\ell_i^{\nu_i}} = \prod\limits_{j\neq i} \ell_j^{\nu_j}$ und erzeugt durch Komposition mit den $\mathsf{P}(\sqrt[\ell_j^{\nu_j}]{a})$ $(j \neq i)$. Die zu $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ gehörige Untergruppe wird also, analog wie vorher, durch *alle* Systeme von Isomorphismen der $\mathsf{P}(\sqrt[\ell_j^{\nu_j}]{a})$ $(j \neq i)$ gebildet. Ganz entsprechend sieht man, daß die dem Teilkörper $\mathsf{P}(\sqrt[\frac{m}{\ell_i^{\nu_i}}]{a})$ zugeordnete Untergruppe durch alle Isomorphismen von $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ gebildet wird. VII, 63

Hieraus geht hervor, daß diejenigen Systeme von Isomorphismen, bei denen jeweils eine bzw. alle bis auf eine Komponente den identischen Isomorphismus erfährt, Untergruppen bilden. Die zugehörigen Teilkörper sind also galoissch, da jeweils *alle* ihre Isomorphismen eine Gruppe bilden, und die Gruppe von $\mathsf{P}(\sqrt[m]{a})$ erscheint als direktes Produkt der Gruppen der $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$.

Da jetzt auch die $\mathsf{P}(\sqrt[\ell_i^{\nu_i}]{a})$ als galoissch erkannt sind, genügt es, den Fall des Primzahlpotenzgrades $m = \ell^\nu$ weiter zu diskutieren, wobei also a keine ℓ–te Potenz ist.

Ist zunächst $\ell \neq 2$, so kann $\mathsf{P}(\sqrt[\ell^\nu]{a})$ schon deshalb nicht galoissch sein, weil sein Grad ℓ^ν nicht durch den Grad $\ell^{\nu-1}(\ell-1)$ des Körpers der ℓ^ν–ten Einheitswurzeln teilbar ist.

Ist ferner $\ell = 2$, so enthält $\mathsf{P}(\sqrt[2^\nu]{a})$ eine primitive 2^ν–te Einheitswurzel ζ_ν. Angenommen, es sei $\nu > 1$. $\mathsf{P}(\sqrt[2^\nu]{a})$ ist dann vom Grade 2 über dem Teilkörper $\mathsf{P}(\zeta_\nu)$ vom Grade $2^{\nu-1}$. Da bei der einzigen nicht–identischen Relativsubstitution S $\sqrt[2^\nu]{a}$ jedenfalls einen Einheitswurzelfaktor ζ_ν^x bekommt, und $\mathsf{S}^2 = 1$ ist, während ζ_ν bei S invariant ist, folgt $\zeta_\nu^{2x} = 1$, $\zeta_\nu^x = -1$, sodaß also $\sqrt[2^{\nu-1}]{a}$ bei S invariant ist. Damit hat man dann $\mathsf{P}(\sqrt[2^{\nu-1}]{a}) = \mathsf{P}(\zeta_\nu)$, und insbesondere ist jetzt auch $\mathsf{P}(\sqrt[2^{\nu-1}]{a})$ als galoissch erkannt. So fortfahrend folgt schließlich, daß $\mathsf{P}(\sqrt{a}) = \mathsf{P}(\zeta_4) = \mathsf{P}(\sqrt{-1})$ ist. Das widerspricht aber der Voraussetzung über a, wonach a mindestens eine Primzahl p mit einem zu 2 primen Exponenten enthält. — VII, 64

Ich nehme jetzt den Beweis des Hauptsatzes auf. Nach der schon angegebenen Wahl von k enthält Ω sicher die Zahlen $\sqrt{p_i}$ (auch falls ein $p_i = 2$ ist) und $\sqrt[\frac{k}{2}]{-1}$ (primitive k–te Einheitswurzel). Ich zeige, daß die Zahlen $-1, p_1, \ldots, p_r$ k–unabhängig in Ω sind. Hätte man nämlich eine Relation VII, 65

$$(-1)^{a_0}\, p_1^{a_1} \cdots p_r^{a_r} = \alpha^k, \quad \alpha \text{ in } \Omega\,,$$

so ist α eine absolut–abelsche Zahl, also $\mathsf{P}(\alpha)$ gewiß galoissch. Da andrerseits

$$\alpha = \sqrt[k]{(-1)^{a_0}\, p_1^{a_1} \cdots p_r^{a_r}}\,,$$

so folgt nach Hilfssatz 2, daß $a_1, \ldots, a_r \equiv 0$ mod. $\frac{k}{2}$ sein müssen, sodaß in der Tat die angenommene Relation zur Folge hat, das jeder Faktor für sich k–te Potenz in Ω ist.

Ich betrachte jetzt den Kummerschen Körper

$$\mathsf{K} = \Omega\left(\sqrt[k]{-1},\ \sqrt[k]{p_1}, \ldots, \sqrt[k]{p_r}\right)\,.$$

Wegen der k–Unabhängigkeit von $-1, p_1, \ldots, p_r$ ist er vom Typus $\left(2, \frac{k}{2}, \ldots, \frac{k}{2}\right)$ über Ω. Es gibt daher ein Primideal $\mathfrak{q}$ vom 1. Grade in Ω, das in bezug auf die Komponenten $\Omega(\sqrt[k]{-1})$, $\Omega(\sqrt[k]{p_1}), \ldots, \Omega(\sqrt[k]{p_r})$ von K zu Frobenius–Substitutio- VII, 66 nen der Ordnungen $2, \frac{k}{2}, \ldots, \frac{k}{2}$ gehört, dessen Primteiler in jenen Komponenten also die Grade $2, \frac{k}{2}, \ldots, \frac{k}{2}$ haben.

Wir betrachten nun die Einteilung nach den k–ten Potenzresten mod. q, wo $q = \mathfrak{N}(\mathfrak{q})$. Die Grade der Primteiler von $\mathfrak{q}$ in den genannten Komponenten sind jeweils die Ordnungen von $-1, p_1, \ldots, p_r$ in bezug auf die Gruppe der k–ten Potenzreste mod. $\mathfrak{q}$, also mod. q, und daher sind diese Ordnungen $2, \frac{k}{2}, \ldots, \frac{k}{2}$, was wegen $k \equiv 0$ mod. $2k_i$, $\frac{k}{2} \equiv 0$ mod. k_i die Behauptung ergibt.

7.19 Beweis der Funktionalgleichung der *L*–Reihen in algebraischen Körpern nach der Schleifenintegralmethode. (Dez. 1932.)

Proof of the functional equation of L-series. Hasse gave this proof in his Seminar on Thursday, Dec 8, 1932 (as he had written to Davenport in a letter of Dec 7). At the end of the present entry Hasse refers to a letter of Siegel of December 5, 1932, concerning the algebraic structure of all proofs of the functional equation. See also the entry 7.28 of February 1934 which is based on a conversation with Artin on this point.]

VII, 67

Dezember 1932.

I. Die verallgemeinerte geometrische Reihe.

Ω sei ein algebraischer Körper vom Grade n und Diskriminantenbetrag d mit r_1 reellen konjugierten (Indizes ν_1) und r_2 Paaren komplexer konjugierter (Indizes ν_2).

t sei ein Vektor (t_ν) der diesen $r_1 + r_2$ Indizes entspricht, und aus positiv reellen Zahlen besteht. Zur Abkürzung:

$$\mathfrak{N}_1(t) = \prod_{\nu_1} t_\nu\,,$$

$$\left.\begin{aligned} \mathfrak{N}(t) &= \prod_\nu t_\nu^{e_\nu} \\ S(t) &= \sum_\nu e_\nu t_\nu \end{aligned}\right\}, \text{wo} \quad e_{\nu_1} = 1\,,\ e_{\nu_2} = 2\,,$$

$\mathfrak{a} = [\alpha_\kappa]$ und $\mathfrak{b} = [\beta_\kappa]$ seien zwei komplementäre Ideale aus Ω, also $\mathfrak{ab} = \frac{1}{\mathfrak{d}}$ die reziproke Differente, dargestellt durch komplementäre Basen,

$$\alpha = \sum_\kappa m_\kappa \alpha_\kappa\,, \quad \beta = \sum_\kappa n_\kappa \beta_\kappa \quad (m_\kappa, n_\kappa \ \text{ganz rat.})$$

Die allgemeinen Zahlen aus ihnen und

$$\xi = \sum_\kappa x_\kappa \alpha_\kappa$$

mit beliebig reellen x_κ. Dann ist $S(\beta\xi) = \sum_\kappa n_\kappa x_\kappa$.

ϱ sei eine beliebige Zahl $\neq 0$ aus Ω, die zur Festlegung einer Signatur sgn ϱ dienen möge. Zur Abkürzung:

VII, 68

$$\varepsilon(\xi) = \begin{cases} 1 & \text{für } \operatorname{sgn}\xi = \operatorname{sgn}\varrho \\ 0 & \text{sonst.} \end{cases}$$

Dann betrachten wir die *verallgemeinerte geometrische Reihe* in Ω:

$$F(t;\, \xi, \mathfrak{a}, \varrho) = \sum_\alpha \varepsilon(\xi+\alpha)\, \mathfrak{N}_1|\xi+\alpha|\, e^{-2\pi S(|\xi+\alpha|t)}.$$

Sie ist periodisch in den x_κ mit den Perioden 1. Sie gestattet daher eine Fourier–Entwicklung (Berechtigungsnachweis durch Poissonsche Summationsformel), die an der Stelle

$$\xi_0 = \sum_\kappa x_\kappa^{(0)} \alpha_\kappa$$

so lautet:

$$F(t;\, \xi_0, \mathfrak{a}, \varrho) = \sum_\beta e^{-2\pi i S(\beta\xi_0)} \int_0^1 \cdots \int F(t;\, \xi, \mathfrak{a}, \varrho)\, e^{2\pi i S(\beta\xi)} dx_\kappa$$

$$= \sum_\beta e^{-2\pi i S(\beta\xi_0)} \int_0^1 \cdots \int \sum_\alpha \varepsilon(\xi+\alpha)\, \mathfrak{N}_1|\xi+\alpha|\, e^{-2\pi[S(|\xi+\alpha|t) - iS(\beta\xi)]} dx_\kappa,$$

also wenn $\sum_\alpha$ mit $\int_0^1 \cdots \int$ vertauscht wird (Berechtigungsnachweis durch Poissonsche Summationsformel):

$$= \sum_\beta e^{-2\pi i S(\beta\xi_0)} \sum_\alpha \int_0^1 \cdots \int \varepsilon(\xi+\alpha)\, \mathfrak{N}_1|\xi+\alpha|\, e^{-2\pi[S(|\xi+\alpha|t) - iS(\beta\xi)]} dx_\kappa$$

$$= \sum_\beta e^{-2\pi i S(\beta\xi_0)} \int_{-\infty}^{+\infty} \cdots \int \varepsilon(\xi)\, \mathfrak{N}_1|\xi|\, e^{-2\pi[S(|\xi|t) - iS(\beta\xi)]} dx_\kappa$$

VII, 69

Jetzt gehen wir von den x_κ durch die Substitution

$$\xi^{(\nu)} = \sum_{\kappa} x_\kappa \alpha_\kappa^{(\nu)} = \left\{ \begin{array}{l} \operatorname{sgn} \varrho^{(\nu)} \cdot u_\nu \\ e^{\pm 2\pi i \varphi_\nu} \cdot u_\nu \end{array} \right\} \quad \left(\begin{array}{l} \text{in leicht verständ-} \\ \text{licher Symbolik} \end{array} \right)$$

mit der Funktionaldeterminante

$$\left| \frac{\partial x_\kappa}{\partial(u_\nu,\, \varphi_\nu)} \right| = \frac{\left| \frac{\partial \xi^{(\nu)}}{\partial(u_\nu,\, \varphi_\nu)} \right|}{\left| \frac{\partial \xi^{(\nu)}}{\partial x_\kappa} \right|} = \frac{(4\pi)^{r_2} \prod_{\nu_2} u_\nu}{\mathfrak{N}\mathfrak{a}\, \sqrt{d}}$$

zu den Variablen u_ν, φ_ν über, die das Gebiet

$$u_\nu \geqq 0\,, \quad 0 \leqq \varphi_\nu \leqq 1$$

bis auf Randmannigfaltigkeiten eineindeutig auf den vollen Raum der x_κ abbilden. Damit wird:

$$\begin{aligned} F(t;\, \xi_0, \mathfrak{a}, \varrho) \quad = \quad & \frac{(4\pi)^{r_2}}{\mathfrak{N}\mathfrak{a}\sqrt{d}} \sum_{\beta} e^{-2\pi i S(\beta\xi_0)} \\ & \cdot \prod_{\nu_1} \int_0^\infty u_\nu e^{-2\pi u_\nu (t_\nu - \operatorname{sgn} \varrho^{(\nu)} \cdot i\beta^{(\nu)})} du_\nu \\ & \cdot \prod_{\nu_2} \int_0^1 \int_0^\infty u_\nu e^{-4\pi u_\nu (t_\nu - i|\beta^{(\nu)}| \cos 2\pi\varphi_\nu)} du_\nu\, d\varphi_\nu \end{aligned}$$

$$= \frac{(4\pi)^{r_2}}{\mathfrak{N}\mathfrak{a}\sqrt{d}} \sum_{\beta} e^{-2\pi i S(\beta\xi_0)} \cdot \prod_{\nu_1} \frac{1}{(2\pi)^2 (t_\nu - \operatorname{sgn} \varrho^{(\nu)} \cdot i\beta^{(\nu)})^2}$$

$$\cdot \prod_{\nu_2} \int_0^1 \frac{d\varphi_\nu}{(4\pi)^2 (t_\nu - i|\beta^{(\nu)}| \cos 2\pi\varphi_\nu)^2}$$

Nun ist

$$\int_0^1 \frac{d\varphi}{(t - ib\cos 2\pi\varphi)^2} = -\frac{d}{dt} \int_0^1 \frac{d\varphi}{t - ib\cos 2\pi\varphi}$$

und für reelles $b > 0$ hat $t - ib\cos 2\pi\varphi$ im oberen Halbperiodenstreifen genau eine Nullstelle φ_0. Es ist dann

$$\int_0^1 \frac{d\varphi}{t - ib\cos 2\pi\varphi} = \int_{\downarrow\, 0 \,\longrightarrow\, 1 \uparrow} \frac{d\varphi}{t - ib\cos 2\pi\varphi}$$

$$= 2\pi i \cdot \text{Residuum des Integranden dort.}$$

Es ist

$$t - ib\cos\varphi = (\varphi - \varphi_0)\cdot\frac{d}{d\varphi}\left(t - ib\cos 2\pi\varphi\right)\Big|_{\varphi_0} + \cdots$$

VII, 70

$$= (\varphi - \varphi_0)\cdot 2\pi ib\sin 2\pi\varphi_0 + \cdots,$$

also das Residuum $= \frac{1}{2\pi ib\sin 2\pi\varphi_0}$ und daher das Integral

$$\int_0^1 \frac{d\varphi}{t - ib\cos 2\pi\varphi} = \frac{1}{b\sin 2\pi\varphi_0} = \frac{1}{b\sqrt{1-\cos^2 2\pi\varphi_0}}$$

$$= \frac{1}{b\sqrt{1+\frac{t^2}{b^2}}} = \frac{1}{\sqrt{t^2+b^2}}\,.$$

Dabei ist das Vorzeichen der Wurzel positiv zu nehmen. Denn für $2\pi\varphi_0 = x + iy$ ist

$$\begin{aligned}
\sin 2\pi\varphi_0 &= \sin x\,\frac{e^y + e^{-y}}{2} + i\cos x\,\frac{e^y - e^{-y}}{2}\\
\cos 2\pi\varphi_0 &= \cos x\,\frac{e^y + e^{-y}}{2} - i\sin x\,\frac{e^y - e^{-y}}{2}\,.
\end{aligned}$$

Ist nun, wie hier, $y > 0$ und $\cos 2\pi\varphi_0$ negativ rein imaginär, so folgt $\cos x = 0$, $\sin x > 0$ (also $x = \frac{\pi}{2}$) und daher $\sin 2\pi\varphi_0 > 0$. — Jetzt folgt endlich

$$\int_0^1 \frac{d\varphi}{(t - ib\cos 2\pi\varphi)^2} = -\frac{d}{dt}\frac{1}{\sqrt{t^2+b^2}} = \frac{t}{\sqrt{t^2+b^2}^{\,3}}\,,$$

und das gilt natürlich auch für $b = 0$.

Damit wird:

VII, 71

$$F(t;\,\xi_0,\mathfrak{a},\varrho)=\frac{1}{(2\pi)^{2r_1}(4\pi)^{r_2}\mathfrak{N}\mathfrak{a}\sqrt{d}}\cdot\sum_{\beta}e^{-2\pi i S(\beta\xi_0)}$$
$$\cdot\prod_{\nu_1}\frac{1}{(t_\nu-\operatorname{sgn}\varrho^{(\nu)}\cdot i\beta^{(\nu)})^2}$$
$$\cdot\prod_{\nu_2}\frac{t_\nu}{\sqrt{t_\nu^2+|\beta^{(\nu)}|^2}^{\,3}}$$

II. Beweis der Funktionalgleichung.

Es sei $L(s,\chi)$ eine L–Reihe des Körpers Ω, gebildet mit einem Charakter χ mod. $\mathfrak{f}$, wo $\mathfrak{f}$ *alle* reellen unendl. Primst. enthält. Dieser Charakter soll *eigentlich* sein, was den endlichen Bestandteil $\mathfrak{f}_0$ von $\mathfrak{f}$ angeht, dagegen braucht der Führer $\mathfrak{f}(\chi)$ nicht notwendig *alle* reellen unendlichen Primstellen zu enthalten. Wir setzen $a_\nu=0$ oder 1, je nachdem die dem ν–ten reellen konjugierten Körper entsprechende Primstelle im Führer von χ nicht vorkommt oder vorkommt.

Es ist

$$L(s,\chi)=\sum_{\mathfrak{K}}\chi(\mathfrak{K})\zeta(s,\mathfrak{K})\,,$$

wo $\mathfrak{K}$ alle Strahlklassen mod $\mathfrak{f}$ durchläuft und

$$\zeta(s,\mathfrak{K})=\sum_{\substack{\mathfrak{m}\sim\mathfrak{r}\,(\mathfrak{f})\\ \mathfrak{n}\text{ ganz}}}\frac{1}{\mathfrak{N}\mathfrak{n}^s}\qquad\begin{matrix}(\mathfrak{r}\text{ ganz aus }\mathfrak{K})\\(\sigma=\Re s>1)\end{matrix}$$

ist.

Sei $\mathfrak{a}_0$ ein ganzes Ideal, prim zu $\mathfrak{f}_0$, für das $\mathfrak{a}_0\mathfrak{K}$ in die absolute Hauptklasse fällt, und $\mathfrak{a}_0\mathfrak{r}=(\varrho)$. Dann wird:

$$\zeta(s,\mathfrak{K})=\mathfrak{N}\mathfrak{a}_0^s\sum_{\substack{\alpha\equiv\varrho\text{ mod.}^+\mathfrak{a}_0\mathfrak{f}_0\\ \operatorname{sgn}\alpha=\operatorname{sgn}\varrho}}^{(\alpha)}\frac{1}{\mathfrak{N}|\alpha|^s}\,,$$

wo $\sum^{(\alpha)}$ anzeigt, daß nur über nicht–assoziierte α zu summieren ist; es genügt aber, wegen der Bedingungen für α, zu sagen: es soll nur über *mod.* $\mathfrak{f}$ *nicht–assoziierte* α summiert werden, wobei „mod $\mathfrak{f}$ assoziiert“ den Zusammenhang

VII, 72

durch eine *Strahleinheit* mod $\mathfrak{f}$ bedeutet. Sind nämlich zwei unserer α überhaupt assoziiert, so auch mod. $\mathfrak{f}$.

Wir setzen nun für $\nu = \nu_1$

$$\frac{\Gamma(s+1)}{(2\pi)^s \left|\alpha^{(\nu)}\right|^s} = 2\pi|\alpha_\nu| \int\limits_0^\infty t_\nu^s \, e^{-2\pi|\alpha^{(\nu)}|t_\nu} dt_\nu \,,$$

für $\nu = \nu_2$

$$\frac{\Gamma(2s)}{(4\pi)^{2s}|\alpha^{(\nu)}|^{2s}} = \int\limits_0^\infty t_\nu^{2s} e^{-4\pi|\alpha^{(\nu)}|t_\nu} \, \frac{dt_\nu}{t_\nu} \,,$$

und erhalten:

$$\frac{\Gamma(s+1)^{r_1}\,\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s+1)}(4\pi)^{r_2 s}\,\mathfrak{N}\mathfrak{a}_0^s}\,\zeta(s,\mathfrak{K})$$

$$= \sum_{\substack{\alpha \equiv \rho \text{ mod.}^+ \mathfrak{a}_0\mathfrak{f}_0 \\ \operatorname{sgn}\alpha = \operatorname{sgn}\rho}}^{(\alpha)} \mathfrak{N}_1|\alpha| \int\limits_0^\infty \cdots \int \mathfrak{N}(t)^s \, e^{-2\pi S(|\alpha|t)} \, dt_{\nu_1} \, \frac{dt_{\nu_2}}{t_{\nu_2}}$$

$$= \int\limits_0^\infty \cdots \int \mathfrak{N}(t)^s \sum_{\substack{\alpha \equiv \rho \text{ mod.}^+ \mathfrak{a}_0\mathfrak{f}_0 \\ \operatorname{sgn}\alpha = \operatorname{sgn}\rho}}^{(\alpha)} \mathfrak{N}_1|\alpha| \, e^{-2\pi S(|\alpha|t)} \, dt_{\nu_1} \, \frac{dt_{\nu_2}}{t_{\nu_2}} \,.$$

Hier führen wir die Substitution aus:

$$t_\nu = \prod_\kappa |\varepsilon_\kappa^{(\nu)}|^{y_\kappa} \cdot z^{\frac{1}{n}}, \quad \text{also} \quad z = \mathfrak{N}(t) \,,$$

VII, 73 wo die ε_κ ein System von Grundeinheiten des Strahls mod $\mathfrak{f}$ sind. Die Funktionaldeterminante berechnet sich aus

$$e_\nu \, \frac{dt_\nu}{t_\nu} = \sum_\kappa e_\nu \log |\varepsilon_\kappa^{(\nu)}| + \frac{e_\nu}{n} \, \frac{dz}{z}$$

$$\left|\frac{\partial t_\nu^\nu}{\partial(y_\kappa, z)}\right| = \frac{1}{2^{r_2}} \mathsf{R}_\mathfrak{f} \cdot \frac{\prod_{\nu_1} t_\nu \prod_{\nu_2} t_\nu}{z} \,,$$

$$\text{wo} \qquad \mathsf{R}_\mathfrak{f} = \left\| e_\nu \log |\varepsilon_\kappa^{(\nu)}| \right\| \qquad \begin{pmatrix} \kappa, \nu = 1, \ldots, r \\ r = r_1 + r_2 - 1 \end{pmatrix}$$

der Regulator des Strahls mod. $\mathfrak{f}$ ist (so normiert, daß $\mathsf{R}_\mathfrak{f} = 1$ für $r = 0$). Und die Abbildung erfolgt bis auf Randmannigfaltigkeiten eineindeutig auf das Gebiet:

$$-\infty < y_\kappa < +\infty\,, \quad z \geqq 0\,.$$

Es wird also:

$$\frac{\Gamma(s+1)^{r_1}\,\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s+1)}(4\pi)^{2r_2 s}\mathfrak{N}\mathfrak{a}_0^s}\,\zeta(s,\mathfrak{K})$$

$$= \frac{\mathsf{R}_\mathfrak{f}}{2^{r_2}}\int\limits_0^\infty z^{s-1}\int\limits_{-\infty}^{+\infty}\!\!\cdots\!\int \mathfrak{N}_1(t)\sum_{\substack{\alpha\,\equiv\,\rho \text{ mod.}^+\mathfrak{a}_0\mathfrak{f}_0\\ \operatorname{sgn}\alpha\,=\,\operatorname{sgn}\rho}}^{(\alpha)} \mathfrak{N}_1|\alpha|\,e^{-2\pi S(|\alpha|t)}\,dy_\kappa dz\,,$$

wobei natürlich im inneren Integral $t = t(y_\kappa, z)$ aufzufassen ist.

Durch Abspalten von Strahleinheitsprodukten von α und Hinzufügen dieser Produkte an t wird dies in bekannter Weise:

$$= \frac{\mathsf{R}_\mathfrak{f}}{2^{r_2}w_\mathfrak{f}}\int\limits_0^\infty z^{s-1}\int\limits_0^1\!\cdots\!\int \mathfrak{N}(t)\sum_{\substack{\alpha\,\equiv\,\rho \text{ mod.}^+\mathfrak{a}_0\mathfrak{f}_0\\ \operatorname{sgn}\alpha\,=\,\operatorname{sgn}\rho}} \mathfrak{N}_1|\alpha|\,e^{-2\pi S(|\alpha|t)}\,dy_\kappa dz\,,$$

wo jetzt über *Zahlen* α statt Hauptideale (α) zu summieren ist; $w_\mathfrak{f}$ bezeichnet die Anzahl der Einheitswurzeln im Strahl mod. $\mathfrak{f}$. Die $\sum_\alpha$ ist jetzt gerade unsere verallgemeinerte geometrische Reihe $F(t;\varrho,\mathfrak{a}_0\mathfrak{f}_0,\varrho)$. Also: VII, 74

$$\frac{\Gamma(s+1)^{r_1}\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s+1)}(4\pi)^{2r_2 s}\mathfrak{N}\mathfrak{a}_0^s}\cdot\frac{2^{r_2}w_\mathfrak{f}}{\mathsf{R}_\mathfrak{f}}\,\zeta(s,\mathfrak{K})$$

$$= \int\limits_0^\infty z^{s-1}\int\limits_0^1\!\cdots\!\int \mathfrak{N}_1(t)\,F(t;\;\varrho,\mathfrak{a}_0\mathfrak{f}_0,\varrho)\,dy_\kappa dz\,,$$

und nach unserer Summenformel, unter Abspaltung des Gliedes $\beta = 0$

$$\frac{\mathfrak{N}\mathfrak{f}_0\sqrt{d}\,\Gamma(s+1)^{r_1}\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s-1)}(4\pi)^{r_2(2s-1)}\mathfrak{N}\mathfrak{a}_0^{s-1}}\cdot\frac{2^{r_2}w_\mathfrak{f}}{\mathsf{R}_\mathfrak{f}}\,\zeta(s,\mathfrak{K})$$

$$= \int\limits_0^\infty z^{s-1}\int\limits_0^1\!\cdots\!\int\left(\frac{1}{z} + \mathfrak{N}_1(t)\sum_\beta{}'\cdots\right)dy_\kappa dz\,,$$

wo $\sum'_\beta$ die auf S. 70 unten angegebene Bedeutung für $\mathfrak{a} = \mathfrak{a}_0\mathfrak{f}_0$, also $\mathfrak{b} = \frac{1}{\mathfrak{a}_0\mathfrak{f}_0\mathfrak{d}}$ hat, aber nur über die $\beta \neq 0$ des Ideals $\frac{1}{\mathfrak{a}_0\mathfrak{f}_0\mathfrak{d}}$ zu summieren ist.

All' das gilt für $\sigma > 1$. Wir zerlegen jetzt das Integral rechts:

$$
\begin{aligned}
= \; & \int_0^1 z^{s-1}\,\frac{dz}{z} \\
& + \int_0^1 z^{s-1} \int_0^1 \cdots \int \mathfrak{N}_1(t) \sum_\beta{}' \cdots \, dy_\kappa dz \\
& + \int_1^\infty z^{s-1} \int_0^1 \cdots \int \left(\frac{1}{2} + \mathfrak{N}_1(t) \sum_\beta{}' \cdots \right) dy_\kappa dz \\
= \; & \frac{1}{s-1} \\
& + \text{für } \sigma > -\frac{1}{2} \text{ reg. Fkt.} \\
& + \text{ganze Funktion.}
\end{aligned}
$$

Daß das zweite Integral für $\sigma > -\frac{1}{2}$ regulär ist, folgt daraus, daß der Integrand an der kritischen Stelle $z = 0$ höchstens wie $z^{\sigma - \frac{1}{2}}$ unendlich wird (man muß natürlich auch das innere Integral dabei berücksichtigen!). Und daß das dritte Integral überall regulär ist, folgt aus dem exponentiellen Verschwinden von $F(t;\, \varrho, \mathfrak{a}_0\mathfrak{f}_0, \varrho)$ für $t \to \infty$.

Hiernach ist $\zeta(s, \mathfrak{K})$ zunächst bis $\sigma > -\frac{1}{2}$ fortgesetzt, und hat dort nur *einen* Pol 1. Ordnung bei $s = 1$ mit dem Residuum $\frac{(2\pi)^{r_2} \mathsf{R}_\mathfrak{f}}{\mathfrak{N}\mathfrak{f}_0 \sqrt{d}\, w_\mathfrak{f}}$.*) VII, 75

Spaltet man jetzt das Glied mit $\beta = 0$ auch im dritten Integral ab, so hört dies zwar auf, ganze Funktion zu sein, aber für $\sigma > -\frac{1}{2}$ gilt jedenfalls die so

*) NB. Das entspr. Resultat, wenn $\mathfrak{f}$ nicht *alle* reellen unendlichen Primstellen enthält, steht in der Vorlesung vom S. S. 1932.

entstehende Relation:

$$\frac{\mathfrak{N}\mathfrak{f}_0\,\sqrt{d}\,\Gamma(s+1)^{r_1}\,\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s-1)}(4\pi)^{r_2(2s-1)}\,\mathfrak{N}\mathfrak{a}_0^{s-1}}\cdot\frac{2^{r_2}w_{\mathfrak{f}}}{\mathsf{R}_{\mathfrak{f}}}\cdot\zeta(s,\mathfrak{K})$$

$$\int\limits_0^\infty z^{s-1}\int\limits_0^1\cdots\int \mathfrak{N}_1(t)\sum_\beta{}'\cdots\,dy_\kappa dz$$

ausführlich:

$$=\int\limits_0^\infty z^{s-1}\int\limits_0^1\cdots\int\sum_\beta{}' e^{-2\pi i S(\beta\varrho)}\prod_{\nu_1}\frac{t_\nu}{(t_\nu-\operatorname{sgn}\varrho^{(\nu)}\cdot i\beta^{(\nu)})^2}$$
$$\cdot\prod_{\nu_2}\frac{t_\nu}{\sqrt{t_\nu^2+|\beta^{(\nu)}|^2}^{\,3}}\,dy_\kappa dz$$
$$=\int\limits_0^\infty z^{s-1}\int\limits_0^1\cdots\int\sum_\beta{}' e^{-2\pi i S(\beta\varrho)}\frac{1}{\mathfrak{N}|\beta|}\prod_{\nu_1}\frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\left(\frac{t_\nu}{|\beta^{(\nu)}|}-\operatorname{sgn}\beta^{(\nu)}\varrho^{(\nu)}\cdot i\right)^2}$$
$$\cdot\prod_{\nu_2}\frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\sqrt{\frac{t_\nu^2}{|\beta^{(\nu)}|^2}+1}^{\,3}}\,dy_\kappa dz\;.$$

Da $S(\beta\varrho)$ nur von der Restklasse $\beta \mod \mathfrak{f}_0$ abhängt und $\operatorname{sgn}\beta^{(\nu)}\varrho^{(\nu)}$ jedenfalls nur von der Restklasse $\beta \mod \mathfrak{f}$, so kann β mit beliebigen Strahleinheiten mod. $\mathfrak{f}$ multipliziert werden, ohne das allgemeine Summenglied zu ändern. Zieht man diese Faktoren wieder zu t, so erhält man in bekannter Weise:

$$=w_{\mathfrak{f}}\int\limits_0^\infty z^{s-1}\int\limits_{-\infty}^{+\infty}\cdots\int\sum_{(\beta)}{}' e^{-2\pi i S(\beta\varrho)}\,\frac{1}{\mathfrak{N}|\beta|}\prod_{\nu_1}\frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\left(\frac{t_\nu}{|\beta^{(\nu)}|}-\operatorname{sgn}\beta^{(\nu)}\varrho^{(\nu)}\cdot i\right)^2}$$
$$\prod_{\nu_2}\frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\sqrt{\frac{t_\nu^2}{|\beta^{(\nu)}|^2}+1}^{\,3}}\,dy_\kappa dz\;,$$

wo jetzt über ein volles System nicht mod. $\mathfrak{f}$ assoziierter Zahlen $\beta\neq 0$ aus dem Ideal $\frac{1}{\mathfrak{a}_0\mathfrak{f}_0\mathfrak{d}}$ zu summieren ist (hier kann aber die Bedingung „mod $\mathfrak{f}$“ bei

VII, 76 „assoziiert“ *nicht* weggelassen werden). Indem man jetzt die y_κ, z in t zurücktransformiert, erhält man weiter:

$$= \frac{w_\mathfrak{f} 2^{r_2}}{\mathsf{R}_\mathfrak{f}} \int_0^\infty \cdots \int \mathfrak{N}(t)^s \sum_{(\beta)}{}' e^{-2\pi i S(\beta\rho)} \frac{1}{\mathfrak{N}|\beta|} \prod_{\nu_1} \frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\left(\frac{t}{|\beta^{(\nu)}|} - \operatorname{sgn}\beta^{(\nu)}\rho^{(\nu)}\cdot i\right)^2}$$

$$\cdot \prod_{\nu_2} \frac{\frac{t_\nu}{|\beta^{(\nu)}|}}{\sqrt{\frac{t_\nu^2}{|\beta^{(\nu)}|^2}+1}^{\,3}} \frac{dt_\nu}{t_\nu}$$

$$= \frac{w_\mathfrak{f} 2^{r_2}}{\mathsf{R}_\mathfrak{f}} \int_0^\infty \cdots \int \mathfrak{N}(t)^s \sum_{(\beta)}{}' e^{-2\pi i S(\beta\rho)} \frac{1}{\mathfrak{N}|\beta|^{1-s}} \prod_{\nu_1} \frac{t_\nu}{\left(t_\nu - \operatorname{sgn}\beta^{(\nu)}\rho^{(\nu)}\cdot i\right)^2}$$

$$\cdot \prod_{\nu_2} \frac{t_\nu}{\sqrt{t_\nu^2+1}^{\,3}} \frac{dt_\nu}{t_\nu},$$

also nach Kürzen beiderseits:

$$\frac{\mathfrak{N}\mathfrak{f}_0\sqrt{d}\,\Gamma(s+1)^{r_1}\Gamma(2s)^{r_2}}{(2\pi)^{r_1(s-1)}(4\pi)^{r_2(2s-1)}\mathfrak{N}\mathfrak{a}_0^{s-1}}\,\zeta(s,\mathfrak{K})$$

$$= \int_0^\infty \cdots \int \sum_{(\beta)}{}' e^{-2\pi i S(\beta\rho)} \frac{1}{\mathfrak{N}|\beta|^{1-s}} \prod_{\nu_1} \frac{t_\nu^s}{\left(t_\nu - \operatorname{sgn}\beta^{(\nu)}\rho^{(\nu)}\cdot i\right)^2}$$

$$\cdot \prod_{\nu_2} \frac{t_\nu^{2s}}{\sqrt{t_\nu^2+1}^{\,3}}\, dt_\nu$$

$$= \sum_{(\beta)}{}' e^{-2\pi i S(\beta\rho)} \frac{1}{\mathfrak{N}|\beta|^{1-s}} \prod_{\nu_1} \int_0^\infty \frac{t_\nu^s}{\left(t_\nu - \operatorname{sgn}\beta^{(\nu)}\rho^{(\nu)}\cdot i\right)^2}\, dt_\nu$$

$$\cdot \prod_{\nu_2} \int_0^\infty \frac{t_\nu^{2s}}{\sqrt{t_\nu^2+1}^{\,3}}\, dt_\nu .$$

Dies gilt für $\sigma > -\frac{1}{2}$, kann aber zu einer für $\sigma < 0$ gültigen Darstellung gemacht

werden, indem man die reellen Integrale durch Schleifenintegrale ersetzt:

$$\int_0^\infty \frac{t^s}{(t \mp i)^2}\,dt = \frac{1}{2i\sin\pi s\, e^{\pi i s}} \int_{\hookrightarrow} \frac{e^{s\log t}}{(t\mp i)^2}\,dt\,,$$

$$\int_0^\infty \frac{t^{2s}}{\sqrt{t^2+1}^{\,3}}\,dt = \frac{1}{2i\sin 2\pi s\, e^{2\pi i s}} \int_{\hookrightarrow} \frac{e^{2s\log t}}{\sqrt{t^2+1}^{\,3}}\,dt\,.$$

Damit ist dann $\zeta(s,\mathfrak{K})$ über die ganze Ebene fortgesetzt, und zwar als für $\sigma < 1$ reguläre Funktion (unter Benutzung der früheren Erkenntnis für $\sigma > -\frac{1}{2}$). Das *erste* Integral läßt sich bequem nach der Schleifenintegralmethode ausrechnen. Man findet: VII, 77

$$\begin{aligned}\int_{\hookrightarrow} \frac{e^{s\log t}}{(t\mp i)^2} &= -\int_{(\pm i)} \frac{e^{s\log t}}{(t\mp i)^2} = -2\pi i \frac{d}{dt} e^{s\log t}\Big|_{\pm i} \\ &= -2\pi i s e^{(s-1)\log(\pm i)} \\ &= -2\pi i s e^{(s-1)(\pi i \mp \frac{\pi i}{2})} \\ &= 2\pi i s e^{\pi i s}\, e^{\mp\frac{\pi i(s-1)}{2}}\,,\end{aligned}$$

somit

$$\int_0^\infty \frac{t^s}{(t\mp i)^2}\,dt = \frac{\pi s}{\sin\pi s}\, e^{\mp\frac{\pi i(s-1)}{2}}$$

und

$$\prod_{\nu_1} \int_0^\infty \frac{t_\nu^s}{(t_\nu - \operatorname{sgn}\beta^{(\nu)}\varrho^{(\nu)}\cdot i)^2}\,dt_\nu = \frac{\pi^{r_1}s^{r_1}}{(\sin\pi s)^{r_1}} \cdot e^{-(r_1 - 2n_{\beta\rho})\frac{\pi i(s-1)}{2}}\,,$$

wo $n_{\beta\rho}$ die Anzahl der negativen unter den reellen konjugierten zu $\beta\rho$ bezeichnet.

Das *zweite* Integral findet man einfacher direkt durch die Substitution $t^2 + 1 = \frac{1}{u}$, $2t\,dt = -\frac{du}{u^s}$, die das Integrationsintervall $0 \leqq t \leqq \infty$ umkehrbar

eindeutig auf $1 \geqq u \geqq 0$ bezieht:

$$\int\limits_0^\infty \frac{t^{2s}}{\sqrt{t^2+1}^{\,3}}\,dt$$

$$= \frac{1}{2}\int\limits_0^1 \frac{\left(\frac{1}{u}-1\right)^s}{\left(\frac{1}{u}\right)^{\frac{3}{2}}}\cdot\frac{1}{\left(\frac{1}{u}-1\right)^{\frac{1}{2}}\,u^2}\,du = \frac{1}{2}\int\limits_0^1 \left(\frac{1}{u}-1\right)^{s-\frac{1}{2}} u^{-\frac{1}{2}}\,du$$

$$= \frac{1}{2}\int\limits_0^1 (1-u)^{s-\frac{1}{2}}u^{-s}\,du = \frac{1}{2}\,\frac{\Gamma(s+\frac{1}{2})\,\Gamma(1-s)}{\Gamma\left(\frac{3}{2}\right)}$$

$$= \frac{\Gamma(s+\frac{1}{2})\,\Gamma(1-s)}{\sqrt{\pi}} = \frac{\Gamma(2s)\,\Gamma(1-s)}{2^{2s-1}\,\Gamma(s)}\,,$$

VII, 78 somit

$$\prod_{\nu_2}\int\limits_0^\infty \frac{t_\nu}{\sqrt{t_\nu^2+1}}\,dt_\nu = \frac{\Gamma(2s)^{r_2}\,\Gamma(s-1)^{r_2}}{2^{r_2(2s-1)}\,\Gamma(s)^{r_2}}\;.$$

Durch Einsetzen dieser Werte und Kürzen erhält man:

$$\frac{\mathfrak{N}\mathfrak{f}_0\sqrt{d}\,(\sin\pi s)^{r_1}\,\Gamma(s)^{r_1}\Gamma(s)^{r_2}}{\pi^{r_1}(2\pi)^{r_1(s-1)}(2\pi)^{r_2(2s-1)}\Gamma(1-s)^{r_2}\,\mathfrak{N}\mathfrak{a}_0^{s-1}}\,\zeta(s,\mathfrak{K})$$

$$= \sum_{(\beta)}{}' e^{-2\pi i S(\beta\varrho)-(r_1-2n_{\beta\varrho})\,\frac{\pi i(s-1)}{2}}\cdot\frac{1}{\mathfrak{N}|\beta|^{1-s}}$$

$$= e^{-r_1\,\frac{\pi i(s-1)}{2}}\sum_{(\beta)}{}' e^{-2\pi i S(\beta\varrho)+n_{\beta\varrho}\pi i(s-1)}\cdot\frac{1}{\mathfrak{N}|\beta|^{1-s}}$$

Multiplizieren wir beiderseits mit $\mathfrak{N}(\mathfrak{a}_0\mathfrak{f}_0\mathfrak{d})^{s-1} = \mathfrak{N}\mathfrak{a}_0^{s-1}\mathfrak{N}\mathfrak{f}_0^{s-1}d^{s-1}$ und setzen $(\beta)\mathfrak{a}_0\mathfrak{f}_0\mathfrak{d} = \mathfrak{n}$, so wird $(\beta\varrho) = \frac{\mathfrak{r}\mathfrak{n}}{\mathfrak{f}_0\mathfrak{d}} = (v)$, und $\mathfrak{n}$ durchläuft alle ganzen Ideale der absoluten Klasse zu $\frac{\mathfrak{f}_0\mathfrak{d}}{\mathfrak{K}}$, während v alle nicht mod. $\mathfrak{f}$ assoziierten Zahlen mit $(v) = \frac{\mathfrak{r}\mathfrak{n}}{\mathfrak{f}_0\mathfrak{d}}$ durchläuft. Somit:

$$\frac{\mathfrak{N}\mathfrak{f}_0^s d^{s-\frac{1}{2}}(\sin\pi s)^{r_1}\,\Gamma(s)^{r_1}\,\Gamma(s)^{r_2}}{\pi^{r_1}\,(2\pi)^{r_1(s-1)}(2\pi)^{r_2(2s-1)}\,\Gamma(1-s)^{r_2}}\,\zeta(s,\mathfrak{K})$$

$$= e^{-r_1\frac{\pi i(s-1)}{2}}\sum_{\mathfrak{n}}\;\sum_{(v)=\frac{\mathfrak{r}\mathfrak{n}}{\mathfrak{f}_0\mathfrak{d}}} e^{-2\pi i S(v)+n_v\pi i(s-1)}\cdot\frac{1}{\mathfrak{N}\mathfrak{n}^{1-s}}$$

Da der Exponent rechts nur von der Restklasse v mod $\mathfrak{f}$ abhängt, kann die Summation über $\mathfrak{n}$ nach den Strahlklassen mod $\mathfrak{f}$ eingeteilt werden (wobei aber auch die *nicht* zu $\mathfrak{f}_0$ primen ganzen Ideale auf die Strahlklassen zu verteilen sind). Durchläuft also $\mathfrak{r}'$ ein volles Repräsentantensystem dieser Strahlklassen, und τ alle nicht mod $\mathfrak{f}$ assoziierten Zahlen mit $(\tau) = \frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}$, so erhält man: VII, 79

$$= e^{-r_1 \frac{\pi i(s-1)}{2}} \sum_{\mathfrak{r}'} \sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}} e^{-2\pi i S(\tau)+n_\tau \pi i(s-1)} \sum_{\substack{u \sim \mathfrak{r}'\,(\mathfrak{f}) \\ \mathfrak{n}\ \text{ganz}}} \frac{1}{\mathfrak{N}\mathfrak{n}^{1-s}}\,.$$

Durch Zusammensetzen der L–Reihe aus den $\zeta(s, \mathfrak{K})$ hat man jetzt:

$$\frac{\mathfrak{N}\mathfrak{f}_0^s d^{s-\frac{1}{2}} (\sin \pi s)^{r_1}\, \Gamma(s)^{r_1} \Gamma(s)^{r_2}}{\pi^{r_1} (2\pi)^{r_1(s-1)}\, (2\pi)^{r_2(2s-1)} \Gamma(1-s)^{r_2}}\, L(s,\chi)$$
$$= e^{-r_1 \frac{\pi i(s-1)}{2}} \sum_{\mathfrak{r},\mathfrak{r}'} \sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)+n_\tau \pi i(s-1)} \sum_{\substack{\mathfrak{n} \sim \mathfrak{r}'\,(\mathfrak{f}) \\ \mathfrak{n}u\ \text{ganz}}} \frac{1}{\mathfrak{N}\mathfrak{n}^{1-s}}\,.$$

Hier durchläuft $\mathfrak{r}$ ein volles Repräsentantensystem der primen Strahlklassen mod $\mathfrak{f}$ und $\mathfrak{r}'$ jedesmal ein volles Repräsentantensystem aller derjenigen (auch nicht primen) Strahlklassen mod $\mathfrak{f}$, für die $\mathfrak{r}\mathfrak{r}' \sim \mathfrak{f}_0\mathfrak{d}$ gilt. Man kann dann auch die Summation nach $\mathfrak{r}'$ voranнehmen, also $\mathfrak{r}'$ *alle* (auch nicht primen) Strahlklassen mod $\mathfrak{f}$ durchlaufen lassen, und $\mathfrak{r}$ dann jedesmal diejenigen primen, für die $\mathfrak{r}\mathfrak{r}' \sim \mathfrak{f}_0\mathfrak{d}$ ist. Dabei ist aber

$$\sum_{\mathfrak{r}} \sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)+n_\tau \pi i(s-1)} = 0 \quad \text{für} \quad (\mathfrak{r}', \mathfrak{f}_0) \neq 1\,.$$

Denn diese Summe bekommt den Faktor $\chi(\gamma)$ für jedes

$$\gamma \equiv 1 \ \text{mod.}\ \frac{\mathfrak{f}}{(\mathfrak{r}', \mathfrak{f}_0)}\,, \quad \gamma \ \text{ prim zu } \mathfrak{f}_0\,,$$

indem $(\gamma)\mathfrak{r}$ und entsprechend $\gamma\tau$ als neue Summationsvariablen eingeführt werden. Weil χ hinsichtlich $\mathfrak{f}_0$ eigentlich vorausgesetzt ist, ist aber nicht jedes zugehörige $\chi(\gamma) = 1$.

Daher ergibt sich:

$$= e^{-r_1 \frac{\pi i(s-1)}{2}} \sum_{\mathfrak{K}'} \sum_{\mathfrak{r}} \sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)+n_\tau \pi i(s-1)} \cdot \zeta(1-s, \mathfrak{K}')\,,$$

VII, 80 wo jetzt $\mathfrak{K}'$ nur alle gewöhnlichen (primen) Strahlklassen mod. $\mathfrak{f}$ durchläuft, $\mathfrak{r}'$ ein Repräsentantensystem der $\mathfrak{K}'$ ist und $\mathfrak{r}$ jedesmal ein Repräsentantensystem derjenigen Strahlklassen mod. $\mathfrak{f}$ durchläuft, die in der absoluten Klasse zu $\frac{\mathfrak{f}_0\mathfrak{d}}{\mathfrak{r}}$ liegen.

Die als Koeffizient von $\zeta(1-s,\mathfrak{K}')$ auftretende Summe ist:

$$e^{-r_1\frac{\pi i(s-1)}{2}}\sum_{\mathfrak{r}}\sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}}\chi(\mathfrak{r})e^{-2\pi iS(\tau)+r_\tau\pi i(s-1)}$$
$$=e^{-r_1\frac{\pi i(s-1)}{2}}\sum_{\mathfrak{s}}e^{\sum_{\nu_1}x_\nu\cdot\pi i(s-1)}\sum_{\mathfrak{r}}\sum_{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}}\chi(\mathfrak{r})\,e^{-2\pi iS(\tau)},$$

wo $\mathfrak{s}=\big((-1)^{x_\nu}\big)$ alle Signaturen durchläuft; bei der Festsetzung $x_\nu=0,1$ ist dann ja $n_\tau=\sum_{\nu_1}x_\nu$ für $\operatorname{sgn}\tau=\mathfrak{s}$. Indem man $(\gamma_\mathfrak{s})\mathfrak{r}$ und dementsprechend $\gamma_\mathfrak{s}\tau$ mit

$$\gamma_\mathfrak{s}\equiv 1\mod\mathfrak{f}_0\,,\quad\operatorname{sgn}\gamma_\mathfrak{s}=\mathfrak{s}$$

als neue Summationsvariable einführt, erhält man weiter:

$$=e^{-r_1\frac{\pi i(s-1)}{2}}\sum_{\mathfrak{s}}e^{\sum_{\nu_1}x_\nu\cdot\pi i(s-1)}\chi(\gamma_\mathfrak{s})\cdot G(\chi,\mathfrak{r}')\,,$$

wo

$$G(\chi,\mathfrak{r}')=\sum_{\mathfrak{r}}\sum_{\substack{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}}\\ \tau\gg 0}}\chi(\mathfrak{r})\,e^{-2\pi iS(\tau)}$$

die (allgemeine) Gausssche Summe zu χ ist.

Stellt man die $\gamma_\mathfrak{s}$ durch eine Basis dar:

$$\gamma_\mathfrak{s}\equiv\prod_{\nu_1}\gamma_\nu^{x_\nu}\mod\mathfrak{f}\,;\quad\operatorname{sgn}\gamma_\nu^{(\nu)}=-1\,,\ \ \operatorname{sgn}\gamma_\nu^{(\nu')}=1\quad(\nu'\neq\nu)\,,$$

VII, 81 und ist

$$\chi(\gamma_\nu)=(-1)^{a_\nu}\qquad(a_\nu=0,1)\,,$$

so wird

$$\chi(\gamma_\mathfrak{s})=(-1)^{\sum_{\nu_1}a_\nu x_\nu}=e^{-\pi i\sum_{\nu_1}a_\nu x_\nu},$$

also unsere Summe weiter:

$$
\begin{aligned}
&= e^{-r_1 \frac{\pi i(s-1)}{2}} \sum_{x_\nu=0}^{1} e^{\pi i \sum_{\nu_1}(s-1-a_\nu)} \cdot G(\chi, \mathfrak{r}') \\
&= e^{-r_1 \frac{\pi i(s-1)}{2}} \prod_{\nu_1} \left(1 - e^{\pi i(s-a_\nu)}\right) \cdot G(\chi, \mathfrak{r}') \\
&= e^{-r_1 \frac{\pi i(s-1)}{2} + \sum_{\nu_1} \frac{\pi i(s-a_\nu)}{2}} (-2i)^{r_1} \prod_{\nu_1} \sin \frac{\pi(s-a_\nu)}{2} \cdot G(\chi, \mathfrak{r}') \\
&= 2^{r_1}\, i^{-\sum_{\nu_1} a_\nu} \prod_{\nu_1} \sin \frac{\pi(s-a_\nu)}{2} \cdot G(\chi, \mathfrak{r}')\,.
\end{aligned}
$$

Hierbei gibt a_ν an, ob die ν–te reelle unendliche Primstelle im Führer $\mathfrak{f}(\chi)$ vorkommt ($a_\nu = 1$) oder nicht ($a_\nu = 0$). Leitet man aus χ einen Zahlcharakter χ_0 und $\mathfrak{f}_0$ durch die Festsetzung ab:

$$\chi_0(\alpha) = \chi(\alpha) \qquad \text{für } \ \alpha \gg 0$$

(und unbeschränkte Fortsetzung mod. $\mathfrak{f}_0$), so wird

$$\chi_0(-1) = (-1)^{\sum_{\nu_1} a_\nu},$$

also

$$i^{\sum_{\nu_1} a_\nu} = \sqrt{\chi_0(-1)} \quad \text{in bestimmter Normierung,}$$

nämlich

$$\sqrt{\chi_0(-1)} = i^{\,p}, \quad \text{wenn } p \text{ unendliche Primstellen in } \mathfrak{f}(\chi) \text{ vorkommen.}$$

So sei fortan $\sqrt{\chi_0(-1)}$ verstanden. VII, 82

Zusammengefaßt wird jetzt:

$$
\sqrt{\chi_0(-1)}\, \frac{\mathfrak{N}\mathfrak{f}_0^s\, d^{s-\frac{1}{2}} (\sin \pi s)^{r_1}\, \Gamma(s)^{r_1} \Gamma(s)^{r_2}}{(2\pi)^{r_1 s} (2\pi)^{r_2(2s-1)} \prod_{\nu_1} \sin \frac{\pi(s-a_\nu)}{2}\, \Gamma(1-s)^{r_2}}\, L(s,\chi)
= \sum_{\mathfrak{K}'} G(\chi, \mathfrak{r}')\, \zeta(1-s, \mathfrak{K}')\,.
$$

VII, 83

Hier wird rechts:

$$G(\chi,\mathfrak{r}') = \sum_{\mathfrak{r}} \sum_{\substack{(\tau)=\frac{\mathfrak{r}\mathfrak{r}'}{\mathfrak{f}_0\mathfrak{d}} \\ \tau\gg 0}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)}$$

$$= \overline{\chi}(\mathfrak{r}') \sum_{\mathfrak{r}} \sum_{\substack{(\tau)=\frac{\mathfrak{r}}{\mathfrak{f}_0\mathfrak{d}} \\ \tau\gg 0}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)} = \overline{\chi}(\mathfrak{r}')\, G(\chi)\,,$$

wo

$$G(\chi) = G(\chi,1) = \sum_{\mathfrak{r}} \sum_{\substack{(\tau)=\frac{\mathfrak{r}}{\mathfrak{f}_0\mathfrak{d}} \\ \tau\gg 0}} \chi(\mathfrak{r})\, e^{-2\pi i S(\tau)}$$

VII, 84 die *reduzierte Gausssche Summe* zu χ ist. Daher bildet sich rechts:

$$= G(\chi) \sum_{\mathfrak{K}'} \chi(\mathfrak{K}')\zeta(1-s,\mathfrak{K}') = G(\chi)L(1-s,\overline{\chi})\ .$$

Links wenden wir noch die Formel an:

$$\frac{\sin \pi s\, \Gamma(s)}{\sin \frac{\pi(s-a_\nu)}{2}} = (-1)^{a_\nu} \pi^{\frac{1}{2}}\, 2^s \frac{\Gamma\left(\frac{s+a_\nu}{2}\right)}{\Gamma\left(\frac{1-s+a_\nu}{2}\right)} \quad (a_\nu = 0,1)\,,$$

also:

$$\frac{(\sin \pi s)^{r_1}\, \Gamma(s)^{r_1}}{\prod_{\nu_1} \sin \frac{\pi(s-a_\nu)}{2}} = \chi_0(-1)\, \pi^{\frac{r_1}{2}} 2^{r_1 s} \prod_{\nu_1} \frac{\Gamma\left(\frac{s+a_\nu}{2}\right)}{\Gamma\left(\frac{1-s+a_\nu}{2}\right)}\ .$$

Damit wird unsere Gleichung nach leichter Umgruppierung links:

$$\frac{\mathfrak{N}\mathfrak{f}_0^{\frac{1}{2}}}{\sqrt{\chi_0(-1)}} \cdot \frac{\left(2^{r_1}\mathfrak{N}\mathfrak{f}_0\, d\right)^{s-\frac{1}{2}}}{(2\pi)^{r_1(s-\frac{1}{2})}\, (2\pi)^{r_2(2s-1)}} \prod_{\nu_1} \frac{\Gamma\left(\frac{s+a_\nu}{2}\right)}{\Gamma\left(\frac{1-s+a_\nu}{2}\right)} \frac{\Gamma(s)^{r_2}}{\Gamma(1-s)^{r_2}}$$
$$= G(\chi)L(1-s,\overline{\chi})\,.$$

Hiernach gilt für die Funktion

$$M(s,\chi) = (\mathfrak{N}\mathfrak{f}\cdot d)^{\frac{s}{2}} \prod_{\nu_1} \frac{\Gamma\left(\frac{s+a_\nu}{2}\right)}{(2\pi)^{\frac{s+a_\nu}{2}}} \cdot \prod_{\nu_2} \frac{\Gamma(s)}{(2\pi)^s} \cdot L(s,\chi)$$

die Funktionalgleichung:

$$M(s,\chi) = \frac{\sqrt{\chi_0(-1)}\, G(\chi)}{\sqrt{\mathfrak{N}\mathfrak{f}_0}}\, M(1-s,\overline{\chi})\,.$$

Dabei ist noch einmal gesagt:

χ ein eigentlicher Charakter mod. $\mathfrak{f}(\chi)$

$\mathfrak{f}_0$ der endliche Bestandteil von $\mathfrak{f}(\chi)$

$\mathfrak{f}$ das um alle reellen unendlichen Primstellen erweiterte $\mathfrak{f}_0$

$\mathfrak{N}\mathfrak{f} = 2^{r_1}\mathfrak{N}\mathfrak{f}_0$ (Restklassenanzahl mod. $\mathfrak{f}$)

$a_\nu = 1$ oder 0, je nachdem die betr. reelle unendliche Primstelle in $\mathfrak{f}(\chi)$ vorkommt oder nicht

χ_0 der zu χ gehörige Zahlcharakter mod. $\mathfrak{f}_0$: $\chi_0(\alpha) = \chi(\alpha)$ für $\alpha \gg 0$

VII, 85

$\sqrt{\chi_0(-1)} = i^{\sum_{\nu_1} a_\nu} = i^p$, wo p die Anzahl der in $\mathfrak{f}(\chi)$ vorkommenden reellen unendlichen Primstellen

$$G(\chi) = \sum_{\mathfrak{r}} \sum_{\substack{(\tau)=\frac{\mathfrak{r}}{\mathfrak{f}_0\mathfrak{d}} \\ \tau \gg 0}} \chi(\mathfrak{r}) e^{-2\pi i S(\tau)}$$ die zu χ gehörige Gausssche Summe

($\mathfrak{r}$ durchläuft ein volles System von (ganzen) Repräsentanten der Strahlklassen mod. $\mathfrak{f}$ aus der absoluten Klasse von $\mathfrak{f}_0\mathfrak{d}$; τ durchläuft alle mod $\mathfrak{f}$ (und dann sogar mod $\mathfrak{f}_0$) nicht assoziierten total positiven Zahlen mit $(\tau) = \frac{\mathfrak{r}}{\mathfrak{f}_0\mathfrak{d}}$).

P. S. Über die algebraische Struktur *aller* Funktionalgleichungsbeweise für L–Reihen siehe Brief von Siegel vom 5. Dezember 1932.

7.20 Ein Satz von Jacobsthal. (Nov. 1932)

Number of solutions of the congruence $ax^2 + bx + c \equiv y^2 \bmod p$ according to Jacobsthal. Already in February 1932 there was an entry on the number of solutions of congruences of a diophantine equation modulo a prime number]. There, the diophantione equation was the (generalized) Fermat equation, while here the equation is of genus 0. The corresponding number of solutions can be extracted from the doctoral thesis of Jacobsthal [Jac07]. *We observe that at the end of November 1932 Hasse gave a colloquium talk at the University of Kiel where he talked about the general problem of estimating the number of solutions of congruences of diophantine equations. It appears that he had written down this entry when he prepared that colloquium talk, although according to Hasse's lecture notes. Jacobsthal's result was not discussed there explicitly.*

VII, 86

(Nach Mitteilung von H. Davenport, November 1932)

Satz. *Die Anzahl der Lösungen von*

$$ax^2 + bx + c \equiv y^2 \mod p$$

ist gleich

$$p - \left(\frac{a}{p}\right) .$$

Beweis. Die fragliche Anzahl ist gleich

$$\sum_x \left(1 + \left(\frac{ax^2 + bx + c}{p}\right)\right) = p + \sum_x \left(\frac{ax^2 + bx + c}{p}\right) ,$$

erstreckt über ein volles Restsystem x mod. p. Nun ist

$$\left(\frac{ax^2 + bx + c}{p}\right) \equiv (ax^2 + bx + c)^{\frac{p-1}{2}} \mod p .$$

Bei Ausführung der Potenzierung rechts nach dem polynomischen Lehrsatz entsteht ein Polynom in x vom Grade $p-1$ mit $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)$ als höchstem Koeffizienten:

$$\left(\frac{ax^2 + bx + c}{p}\right) \equiv \left(\frac{a}{p}\right) x^{p-1} + A_1 x^{p-2} + \cdots + A_{p-1} \mod p .$$

Da
$$\sum_x x^n \equiv \left\{ \begin{array}{cc} p-1 \equiv -1 & \text{für } \; p-1|n \\ 0 & \text{sonst} \end{array} \right\} \bmod p\,,$$
folgt in der Tat
$$\sum_x \left(\frac{ax^2+bx+c}{p}\right) \equiv -\left(\frac{a}{p}\right) \text{ mod. } p\,.$$
Hier muß die Gleichheit statt der Kongruenz gelten, da die Summe dem Betrage nach höchstens p und für quadratfreies ax^2+bx+c zudem notwendig ungerade ist.

7.21 Zur „Theorie II“ in der komplexen Multiplikation. (Nov. 1932)

Comments by Artin on Hasse's second paper on complex multiplication [Has31]. *It appears that Artin and Hasse had talked about this paper during Hasse's visit to Hamburg which took place at the end of November 1932. While Hasse's first paper on complex multiplication* [Has26b] *assumed the basic properties of class field theory, the second paper derived those properties in the case of imaginary quadratic base fields by analytic means. The notations in this entry are taken from Hasse's second paper. Artin's comments appear to lead to a simplification of the proof that the singular invariants are abelian over the corresponding imaginary quadratic field. We remark that some weeks later Artin wrote a letter to Hasse explaining that there was an error in Hasse's paper in the proof of the principal ideal theorem. That error could be corrected much later only, in 1959 by Reichardt. See* [FR08], 47.1.

VII, 87

(Bemerkungen von E. Artin, November 1932)

1.) *Beweis, daß* $\varphi_{\mathsf{P}}(\alpha_1, \alpha_2)$, $\varphi_{\overline{\mathsf{P}}}(\alpha_1, \alpha_2)$ *(und ebenso* $\psi_{\mathsf{P}}(\alpha_1, \alpha_2)$, $\psi_{\overline{\mathsf{P}}}(\alpha_1, \alpha_2)$ *— 12. Wurzeln) im Körper* $\mathsf{K} = \Omega\big(j(\mathfrak{k})\big)$ *liegen.*

Wenn festgestellt ist, daß die $\varphi_{\mathsf{P}_\nu}(w_1, w_2)$ (bzw. $\psi_{\mathsf{P}_\nu}(w_1, w_2)$ einer Gleichung $\Phi_p\big(t, j(\mathfrak{w})\big)$ (bzw. $\Psi_p\big(t, j(\mathfrak{w})\big)$ genügen deren Zahlkoeffizienten ganzrational sind, und daß im singulären Falle die von den genannten verschiedenen Wurzeln Einheiten sind, während die beiden genannten Hauptidealdarstellungen von $\mathfrak{p}^{12}$, $\overline{\mathfrak{p}}^{12}$ (bzw. $\mathfrak{p}$, $\overline{\mathfrak{p}}$) sind, so schließe man so:

Der in K irreduzible Faktor von $\Phi_p\big(t, j(\mathfrak{k})\big)$, dem $\varphi_{\mathsf{P}}(\alpha_1, \alpha_2)$ genügt, hat bezgl. K konjugierte Wurzeln. Da $\Omega \leqq \mathsf{K}$, müssen also die anderen Wurzeln notwendig auch Hauptidealdarstellungen von $\mathfrak{p}^{12}$ sein, und das trifft für keine zu. — Entsprechend für $\psi_{\mathsf{P}}(\alpha_1, \alpha_2)$.

2.) Jetzt folgt das gleiche für $\varphi_M(\alpha_1, \alpha_2)$, $\Psi_M(\alpha_1, \alpha_2)$, wenn der Transformationsgrad M aus nach 1.) zulässigen Primzahlen zusammengesetzt ist, einfach durch Zerspaltung in Multiplikatoren von Primzahlgrad. — *Anwendung beim Hauptidealsatz!*

VII, 88

3.) *Beweis des Isomorphiesatzes.*

a.)
$$\delta_{\mathsf{P}}(\alpha_1, \alpha_2) = j^p(\alpha_1, \alpha_2) - j\big(\mathsf{P}(\alpha_1, \alpha_2)\big)$$

liegt nach 1.) in K, da rationalzahlig durch $\varphi_{\mathsf{P}}(\alpha_1, \alpha_2)$, $j(\alpha_1, \alpha_2)$ dargestellt.

Daher liegt auch $j\big(\mathsf{P}(\alpha_1, \alpha_2)\big)$ in K. Durch Iteration folgt daraus sofort, daß $H(t)$ *galoissch* ist. (Die Theorie von $H(t)$ muß natürlich in Theorie II zunächst entwickelt werden.)

b.) Ferner sei gemäß 1.)

$$\varphi_{\mathsf{P}}(\alpha_1, \alpha_2) = \mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{a})\big)\,,$$

wo das Polynom $\mathsf{R}_{\mathfrak{a}}$ Koeffizienten in Ω hat und möglicherweise von $\mathfrak{a}$ abhängt. Dann ist

$$\Phi_p\Big(\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{a})\big), j(\mathfrak{a})\Big) = 0\,,$$

also wegen der Irreduzibilität von $H(t)$ auch

$$\Phi_p\Big(\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{b})\big), j(\mathfrak{b})\Big) = 0\,,$$

d. h. $\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{b})\big)$ ist Wurzel von $\Phi_p\big(t,\, j(\mathfrak{b})\big)$. Als Konjugierte zu $\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{a})\big)$ bezgl. Ω ist auch $\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{b})\big)$ Hauptidealdarstellung von $\mathfrak{p}^{12}$, also notwendig mit der einzigen solchen Wurzel von $\Phi_p\big(t, j(\mathfrak{b})\big)$ identisch:

$$\mathsf{R}_{\mathfrak{a}}\big(j(\mathfrak{b})\big) = \mathsf{R}_{\mathfrak{b}}\big(j(\mathfrak{b})\big).$$

Daher ist genauer

$$\varphi_{\mathsf{P}}(\alpha_1, \alpha_2) = \mathsf{R}_{\mathfrak{b}}\big(j(\mathfrak{b})\big)$$

mit von $\mathfrak{a}$ unabhängigem Polynom R zu Ω. VII, 89

Auf dem Wege über die (von $\mathfrak{a}$ unabhängige) Darstellung von $\delta_{\mathsf{P}}(\alpha_1, \alpha_2)$ durch $\varphi_{\mathsf{P}}(\alpha_1, \alpha_2)$, $j(\alpha_1, \alpha_2)$ folgt jetzt auch

$$j\left(\frac{\mathfrak{a}}{\mathfrak{p}}\right) = j\big(\mathsf{P}(\alpha_1, \alpha_2)\big) = \mathsf{R}^*\big(j(\mathfrak{a})\big)$$

mit von $\mathfrak{a}$ unabhängigem Polynom R^*.

Das ergibt in bekannter Weise, daß K *abelsch* ist und zur Klassengruppe isomorphe Galoisgruppe hat.

7.22 Elementarer Beweis des verallgemeinerten Artinschen Lemmas. (Okt. 1933)

Here Hasse reproduces an elementary proof by van der Waerden of his generalization of Artin's lemma; for the latter see the 7.18.] This proof is published 1933 in Crelle's Journal [vdW34]. *As van der Waerden mentions in the introduction to his paper, the use of multiplicative characters is due to Hasse.*

VII, 90

Nach v. d. Waerden, Oktober 1933

Auf S. 29] wurde elementar bewiesen: *Ist eine natürliche Zahl* $a > 1$ *und eine Primzahlpotenz* ℓ^ν ($\nu \geqq 0$; *für* $\ell = 2$ *sogar* $\nu \geqq 1$) *gegeben, so gibt es eine Primzahl* $p \neq \ell$ *mit*

$$a^{\ell^\nu} \not\equiv 1 \text{ mod. } p\,, \quad a^{\ell^{\nu+1}} \equiv 1 \text{ mod. } p\,.$$

VII, 91

Es ist dann $\ell^{\nu+1} | p-1$, und für jeden ℓ–Charakter χ mod. p mindestens von der Ordnung $\ell^{\nu+1}$ gilt

$$\chi(a)^{\ell^\nu} \neq 1\,, \quad \chi(a)^{\ell^{\nu+1}} = 1\,.$$

Ersetzt man ν durch $\nu+1$, $\nu+2, \ldots$, und χ durch χ^ℓ, $\chi^{\ell^2}, \ldots$, so sieht man, daß es zu a und ℓ^ν auch *unendlich viele* Primzahlen $p \neq \ell$ gibt, sodaß jedesmal für jeden ℓ–Charakter χ mod. p mindestens von der Ordnung $\ell^{\nu+1}$ gilt

$$\chi(a)^{\ell^\nu} \neq 1\,, \quad \chi(a)^{\ell^{\nu+1}} = 1\,.$$

Seien jetzt natürliche Zahlen $a_1, \ldots, a_r > 1$ und ℓ^ν wie bisher gegeben. Dann sei irgendein $\omega \geqq 1$ gewählt (das nachher hinreichend groß festgelegt wird), und dann gemäß obigem Primzahlen $p_1, \ldots, p_r$ und ℓ–Charaktere $\chi_1, \ldots, \chi_r$ zu ihnen so bestimmt, daß

$$\chi_\rho(a_\rho)^{\ell^{\nu+\omega-1}} \neq 1\,, \quad \chi_\rho(a_\rho)^{\ell^{\nu+\omega}} = 1 \tag{1}$$

wird. Dabei seien noch die p_ρ verschieden von den Primteilern der $a_1, \ldots, a_r$ gewählt, was geht, da jedesmal unendlich viele zur Verfügung stehen.

Jetzt werde angesetzt:

$$\chi(x) = \prod_\rho \chi_\rho(x)^{c_\rho}$$

mit zu bestimmenden ganzen c_ρ mod. ℓ^{ν_ρ}, wo ℓ^{ν_ρ} die Ordnung von χ_ρ ist. Wir fordern VII, 92

$$\chi(a_\kappa)^{\ell^\nu} \neq 1\,, \quad (\kappa = 1, \ldots, r)\,. \tag{2}$$

$(2.)_\kappa$ ist verletzt dann und nur dann, wenn

$$\overline{(2.)_\kappa} \qquad \prod_\rho \chi_\rho(a_\kappa)^{c_\rho \ell^\nu} = 1\,, \quad \text{d. h.} \quad \chi_\kappa(a_\kappa)^{c_\kappa \ell^\nu} = \prod_{\rho\neq\kappa} \chi_\rho(a_\kappa)^{-c_\rho \ell^\nu}$$

Zu gegebener c_ρ $(\rho \neq \kappa)$ bestimmt diese Relation entweder eindeutig ein c_κ mod. ℓ^ω, wenn nämlich die rechte Seite eine ℓ^ω–te Einheitswurzel ist — $\chi_\kappa(a_\kappa)^{\ell^\nu}$ ist nach (1) *primitive* ℓ^ω–te Einheitswurzel —, oder ist durch kein c_κ erfüllt, wenn nämlich die rechte Seite von höherer Ordnung als ℓ^ω ist. $\overline{(2.)_\kappa}$ ist also höchstens für $\ell^{\nu_\kappa - \omega}$ Restklassen c_κ mod. ℓ^{ν_κ} erfüllt, bei willkürlich gegebene Restklassen c_ρ mod. ℓ^{ν_ρ} $(\rho \neq \kappa)$, d. h. höchstens für

$$\ell^{\nu_\kappa - \omega} \prod_{\rho\neq\kappa} \ell^{\nu_\rho} = \frac{1}{\ell^\omega} \prod_\rho \ell^{\nu_\rho}$$

der zulässigen $\prod\limits_\rho \ell^{\nu_\rho}$ Systeme c_ρ mod. ℓ^{ν_ρ}. Für höchstens soviele ist also $(2.)_\kappa$ verletzt. Daher ist (2) insgesamt für höchstens $\frac{r}{\ell^\omega} \prod_\rho \ell^{\nu_\rho}$ Systeme c_ρ mod. ℓ^{ν_ρ} verletzt. Wählt man also ω so groß, daß $\ell^\omega > r$ ist, so sind das weniger als alle zulässigen $\prod_\rho \ell^{\nu_\rho}$ Systeme, d. h. es gibt dann mindestens ein System c_ρ, bei dem χ die Bedingungen (2) erfüllt.

χ definiert dann eine zyklische ℓ–Klasseneinteilung (nach dem kl. gem. Vielf. der p_ρ als Modul), bei der die a_ρ mindestens die Ordnung $\ell^{\nu+1}$ haben.

Ist $\ell = 2$, so kann auch noch $\chi(-1) = -1$ erreicht werden. Denn ist $\chi(-1) = 1$, so wähle man ein $p_{r+1} \equiv -1$ mod. 4, das von den Primteilern der a_ρ verschieden ist (existiert als Teiler von $4a, \ldots, a_r - 1$) und setze VII, 93

$$\chi^*(x) = \chi(x) \left(\frac{x}{p_{r+1}}\right).$$

Dann ist

$$\chi^*(-1) = \left(\frac{-1}{p_{r+1}}\right) = -1$$

und

$$\chi^*(a_\rho)^{2^\nu} = \chi(a_\rho)^{2^\nu} \neq 1\,, \quad (\nu \geqq 1)\,.$$

Ist jetzt $k = \prod \ell^\nu$ statt ℓ^ν gegeben und o. B. d. A. gleich k durch 2^2 teilbar, so wähle man für jeden Primteiler ℓ von k einen ℓ–Charakter χ_ε derart, daß

$$\chi_\ell(a_\rho)^{\ell^{\nu-1}} \neq 1\,,\ (\rho = 1, \dots, r)\,; \quad \chi_2(-1) = -1$$

Dann hat

$$\chi = \prod_{\ell | k} \chi_\ell$$

die Eigenschaften

$$\chi(a_\rho) \textit{ hat durch } k \textit{ teilbare Ordnung;} \quad \chi(-1) = -1\,.$$

Damit ist das verallgemeinerte Artinsche Lemma elementar bewiesen.

VII, 94
VII, 95 **Die Seiten 94 und 95 im Tagebuch fehlen.**

7.23 Wittscher Beweis eines Satzes über verschränkte Produkte. (Nov. 1934)

Witt's proof of a result on crossed products; see also 7.16.] Witt published this 1935 in Crelle's Journal [Wit35b].

VII, 96

November 1934

Es handelt sich um den Satz auf S. 49].
Wir haben die erzeugenden Relationen:

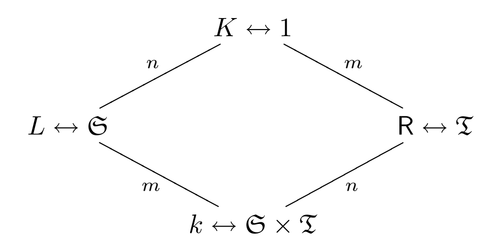
$$xu_{\mathsf{S}} = u_{\mathsf{S}} x^{\mathsf{S}} \qquad xu_{\mathsf{T}} = u_{\mathsf{T}} x^{\mathsf{T}}$$
$$u_{\mathsf{S}} u_{\mathsf{S}'} = u_{\mathsf{SS}'} a_{\mathsf{S},\mathsf{S}'} \qquad u_{\mathsf{T}} u_{\mathsf{T}'} = u_{\mathsf{TT}'} c_{\mathsf{T},\mathsf{T}'}$$

$$u_{\mathsf{T}} u_{\mathsf{S}} = u_{\mathsf{S}} u_{\mathsf{T}} b_{\mathsf{S},\mathsf{T}}$$

eines verschränkten Produkts A zu einem Körper K (Elemente x), dessen Gruppe direktes Produkt aus zwei Gruppen $\mathfrak{S}$ (Elemente S) und $\mathfrak{T}$ (Elemente T) ist.

Behauptung: $A^n \sim (c^{\sum}_{\mathsf{T},\mathsf{T}'}, L)$,

wo L *der Invariantenkörper von* $\mathfrak{S}$
$\sum$ *die Summe aller* S *aus* $\mathfrak{S}$
n *die Anzahl aller* S *aus* $\mathfrak{S}$ *(Ordnung von* $\mathfrak{S}$*)*



Beweis. Einführung neuer Operatoren: VII, 97

$$v_{\mathsf{S}} = u_{\mathsf{R}}^{-1} u_{\mathsf{RS}} \qquad v_{\mathsf{T}} = u_{\mathsf{R}}^{-1} u_{\mathsf{T}} u_{\mathsf{R}} \quad (\mathsf{R} \text{ fest in } \mathfrak{S})$$

Dann ersichtlich auch

$$xv_{\mathsf{S}} = v_{\mathsf{S}} x^{\mathsf{S}} \qquad xv_{\mathsf{T}} = v_{\mathsf{T}} x^{\mathsf{T}},$$

letzteres da R mit T vertauschbar. Ferner hat man also zugeordnetes Faktorensystem:

$$\begin{aligned}
\bar{a}_{\mathsf{S},\mathsf{S}'} = v_{\mathsf{SS}'}^{-1} v_{\mathsf{S}} v_{\mathsf{S}'} &= u_{\mathsf{RSS}'}^{-1} \underbrace{u_{\mathsf{R}} \cdot u_{\mathsf{R}}^{-1}} u_{\mathsf{RS}} \underset{\wedge}{\cdot} u_{\mathsf{R}}^{-1} u_{\mathsf{RS}'} \\
&= \underbrace{u_{\mathsf{RSS}'}^{-1} u_{\mathsf{RS}} u_{\mathsf{S}'}} \underbrace{u_{\mathsf{S}'}^{-1} u_{\mathsf{R}}^{-1} u_{\mathsf{RS}'}} \\
&= \qquad a_{\mathsf{RS},\mathsf{S}'} \qquad a_{\mathsf{R},\mathsf{S}'}^{-1} \\
\bar{b}_{\mathsf{S},\mathsf{T}} = v_{\mathsf{T}}^{-1} v_{\mathsf{S}}^{-1} v_{\mathsf{T}} v_{\mathsf{S}} &= u_{\mathsf{R}}^{-1} u_{\mathsf{T}}^{-1} u_{\mathsf{R}} \underset{\wedge}{\cdot} u_{\mathsf{RS}}^{-1} \underbrace{u_{\mathsf{R}} \cdot u_{\mathsf{R}}^{-1}} u_{\mathsf{T}} \underbrace{u_{\mathsf{R}} \cdot u_{\mathsf{R}}^{-1}} u_{\mathsf{RS}} \\
&= \underbrace{u_{\mathsf{R}}^{-1} u_{\mathsf{T}}^{-1} u_{\mathsf{R}} u_{\mathsf{T}}} \cdot \underbrace{u_{\mathsf{T}}^{-1} u_{\mathsf{RS}}^{-1} u_{\mathsf{T}} u_{\mathsf{RS}}} \\
&= \qquad b_{\mathsf{R},\mathsf{T}}^{-1} \qquad\qquad b_{\mathsf{RS},\mathsf{T}} \\
\bar{c}_{\mathsf{T},\mathsf{T}'} = v_{\mathsf{TT}'}^{-1} v_{\mathsf{T}} v_{\mathsf{T}'} &= u_{\mathsf{R}}^{-1} (u_{\mathsf{TT}'}^{-1} u_{\mathsf{T}} u_{\mathsf{T}'}) u_{\mathsf{R}} = c_{\mathsf{T},\mathsf{T}'}^{\mathsf{R}} \,.
\end{aligned}$$

Durch Multiplikation über alle R aus $\mathfrak{S}$ ergibt sich ein Faktorensystem für A^n, und dieses hat die Form:

$$a^*_{\mathsf{S},\mathsf{S}'} = \prod_{\mathsf{R}} \bar{a}_{\mathsf{S},\mathsf{S}'} = 1\,, \quad b^*_{\mathsf{S},\mathsf{T}} = \prod_{\mathsf{R}} \bar{b}_{\mathsf{S},\mathsf{T}} = 1\,, \quad c^*_{\mathsf{T},\mathsf{T}'} = c^{\Sigma}_{\mathsf{T},\mathsf{T}'} \,.$$

Daraus liest man die Behauptung ab.

7.24 Beweis der Residuennormalform zyklischer Algebren vom Primzahlgrad *p* bei Charakteristik *p*. (Feb. 1935)

Witt's residue formula applies to cyclic algebras of degree p over a power series field with a perfect field of constants. It is contained in Witt's paper on the existence theorem of class field theory for function fields [Wit35a]. *However Witt does not give a proof there. Instead, he says that the proof is essentially the same as the proof by H.L.Schmid of the residue formula for the norm symbol of cyclic extensions of degree p over power series fields* [Sch35]. *It appears that Hasse wished to write down Witt's proof explicitly although, of course, he was familiar with H.L.Schmid's thesis which he had supervised.*

VII, 98

Nach E. Witt, Februar 1935

Hilfssatz 1. *Sei A eine Algebra über k mit den Multiplikationskonstanten*

$$\mathfrak{C} = \left(\gamma_{ik}^{\ell}\right)$$

in bezug auf eine Basis $(e_i) = \mathfrak{e}$. Allgemein werde die Wirkung einer Basistransformation $\mathfrak{e} \to \mathsf{P}\mathfrak{e}$ auf $\mathfrak{C}$ mit $\mathfrak{C} \to \mathfrak{C}^{\mathsf{P}}$ bezeichnet.

Sei dann bekannt, daß bei einem Automorphismus σ von k gilt:

$$\mathfrak{C}^{\sigma} = \mathfrak{C}^{\mathsf{S}}$$

wo S eine Basistransformation ist. Dann gilt:

$$(\mathfrak{C}^{\mathsf{P}})^{\sigma} = (\mathfrak{C}^{\mathsf{P}})^{\mathsf{P}^{-1}\mathsf{S}\mathsf{P}^{\sigma}}.$$

Wenn also bei einer Erzeugung $\mathfrak{C}$ von A die Anwendung des Automorphismus σ die Algebra A nicht ändert, so gilt dies bei jeder Erzeugung $\mathfrak{C}^{\mathsf{P}}$ von A.

Beweis.

$$(\mathfrak{C}^{\mathsf{P}})^{\sigma} = (\mathfrak{C}^{\sigma})^{\mathsf{P}^{\sigma}} = \mathfrak{C}^{\mathsf{S}\mathsf{P}^{\sigma}} = \mathfrak{C}^{\mathsf{P}\mathsf{P}^{-1}\mathsf{S}\mathsf{P}^{\sigma}} = (\mathfrak{C}^{\mathsf{P}})^{\mathsf{P}^{-1}\mathsf{S}\mathsf{P}^{\sigma}}.$$

Hilfssatz 2. *Sei k ein Körper der Charakteristik p und*

$$A = (\alpha, \beta) = k(u, v)$$

die durch

$$\wp u = u^p - u = \alpha\,, \quad v^p = \beta \neq 0 \quad vu = (u+1)v$$

definierte zyklische Algebra über k. Dann gilt für beliebiges y aus $k(v)$ die Formel

$$\wp(u+y) = \wp(u) + \operatorname{Sp} y = \alpha + \operatorname{Sp} y$$

VII, 99 *wo*

$$\operatorname{Sp} y = (\eta_0^p - \eta_0) + \eta_1^p \beta + \cdots + \eta_{p-1}^p \beta^{p-1},$$

wenn

$$y = \eta_0 + \eta_1 v + \cdots + \eta_{p-1} v^{p-1} \quad (\eta_i \ \text{ aus } \ k)\,.$$

Beweis. Setzt man $\overline{u} = u + y$, so gilt auch

$$v\overline{u} = (\overline{u}+1)v\,.$$

Hiernach ist $k(\overline{u})$ ein komm. Teilsystem von A mit den p verschiedenen Automorphismen $\overline{u} \to \overline{u} + \nu \quad (\nu = 0, 1, \ldots, p-1)$. Die Hauptgleichung für $\overline{u}$, die den Grad p hat, hat also die p verschiedenen Wurzeln $\overline{u} + \nu$, und ist somit von der Form

$$\wp\overline{u} = \overline{\alpha}$$

mit $\overline{\alpha}$ in k.

Um $\overline{\alpha}$ zu berechnen, genügt es durch sukzessives Vorgehen, nur den Fall $y = \eta v^\nu$ zu betrachten ($\nu = 0, 1, \ldots, p-1$). Für $\nu = 0$ ist natürlich

$$\wp(u+\eta) = \wp u + \wp\eta = \alpha + (\eta^p - \eta)\,,$$

wie behauptet.

Für $\nu = 1, \ldots, p-1$ ist $\overline{\alpha}$ die reduzierte Norm von $\overline{u}$; als solche berechnet sich VII, 100 $\overline{\alpha}$ als Determinante der Matrix $M_{\overline{u}}$ aus der absolut–irreduziblen Darstellung. Mit $1, v^\nu, v^{2\nu}, \ldots, v^{(p-1)\nu}$ als Basis lautet diese:

$$M_u = \begin{pmatrix} u & & & \\ & u+\nu & & \\ & & \ddots & \\ & & & u+(p-1)\nu \end{pmatrix}\,, \quad M_{v^\nu} = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \ddots & \\ \beta^\nu & & & 1 \end{pmatrix}$$

Für $\overline{u} = u + \eta v^\nu$ wird

$$M_{\overline{u}} = M_u + \eta\, M_{v^\nu} = \begin{pmatrix} u & \eta & & & \\ & u+\nu & \eta & & \\ & & \ddots & & \\ & & & \ddots & \eta \\ \eta\beta^\nu & & & & u+(p-1)\nu \end{pmatrix}$$

und daraus

$$\overline{\alpha} = n(\overline{u}) = |M_{\overline{u}}| = \wp u + \eta^p \beta^\nu = \alpha + \operatorname{Sp} \eta v^\nu,$$

wie behauptet.

Hilfssatz 3. $(\alpha, \beta) \sim k \longleftrightarrow \alpha = \operatorname{Sp} y$ *mit* y *aus* $k(v)$.

Beweis. a.) Sei $\alpha = \operatorname{Sp} y$. Dann setze man

$$\overline{u} = u - y$$

und erhält

$$A = (\alpha, \beta) = k(\overline{u}, v)$$

mit (Hilfssatz 2)

$$\wp\overline{u} = \wp u - \operatorname{Sp} y = \alpha - \alpha = 0\,, \quad v^p = \beta\,, \quad v\overline{u} = (\overline{u}+1)v\,,$$

d. h.

$$A = (0, \beta) \sim k\,.$$

b.) Sei $(\alpha, \beta) \sim k$, also $(\alpha, \beta) = (0, \beta)$. Der zweiten zyklischen Darstellung entsprechend hat man in $A = (\alpha, \beta)$ Elemente $\overline{u}$, $\overline{v}$ mit

$$\wp\overline{u} = 0\,, \quad \overline{v}^p = \beta\,, \quad \overline{v}\,\overline{u} = (\overline{u}+1)\overline{v}\,.$$

Ohne Einschränkung darf A einem solchen inneren Automorphismus unterworfen werden, daß $\overline{v} = v$ gilt.*) Dann ist $u - \overline{u} = y$ mit v vertauschbar, also in $k(v)$, d. h. VII, 101

$$u = \overline{u} + y\,,$$
$$\alpha = \wp u = \wp\overline{u} + \operatorname{Sp} y = \operatorname{Sp} y\,.$$

*) Falls $\beta = \beta_0^p$ in k ist, ist die Behauptung $\alpha = \operatorname{Sp} y$ trivial:

$$\alpha = (-\alpha)^p - (-\alpha) + \left(\frac{\alpha}{\beta_0}\right)^p \beta$$

Sei jetzt k der Körper aller Potenzreihen in π über einem vollkommenen Konstantenkörper k_0 der Charakteristik p:

$$k = \overline{k_0(\pi)}\,.$$

Hilfssatz 4. *Ist* α_0 *in* k_0, β *Einheit in* k, *so ist* $(\alpha_0, \beta) \sim k$.

Beweis. Bekanntlich ist dann $\beta = n(x)$ mit x aus $k(u)$ mit $\wp u = \alpha_0$

Hilfssatz 5. *Invarianz des Residuums* $\rho(\alpha\, d\beta)$ *für* α, β *aus* k *bei den Automorphismen* $\pi \to \pi^\sigma = \varepsilon\pi$ $\quad$ *(*ε *Einheit aus* k*) von* k.

Beweis siehe meine Arbeit in Crelle **172** über Differentiale.

Hauptsatz. $\qquad (\alpha, \beta) = \left(\rho\left(\alpha\,\dfrac{d\beta}{\beta}\right), \pi\right).$

Beweis. **1.)** Sei zunächst $\beta = \pi$. Dann bleibt (α, β) ungeändert, wenn α additiv um einen beliebigen Ausdruck der Form

$$\wp\xi_0 + \xi_1^p\pi + \cdots + \xi_{p-1}^p\pi^{p-1}, \quad \xi_i \text{ in } k$$

VII, 102 abgeändert wird. Sei

$$\alpha = \sum_{\nu=0}^{-n} \frac{a_\nu}{\pi^\nu} + \alpha_1\,, \quad \alpha_1 \equiv 0 \text{ mod. } \pi\,,$$

dann ist

$$\begin{aligned} \alpha_1 &= (\alpha_1 - \alpha_1^p) + (\alpha_1^p - \alpha_1^{p^2}) + \cdots \\ &= -\wp(+\alpha_1 + \alpha_1^p + \cdots)\,, \end{aligned}$$

da $+\alpha_1 + \alpha_1^p + \cdots$ konvergiert. Ferner ist für $\nu = \nu_0 p$:

$$\frac{a_\nu}{\pi^\nu} = \frac{a_\nu^{p-1}}{\pi^{\nu_0}} + \wp\left(\frac{a_\nu^{p-1}}{\pi^{\nu_0}}\right).$$

Außer dem Bestandteil α_1 können hiernach auch alle Glieder mit $\nu \equiv 0 \mod p$ sukzessive aus α durch Hinzufügen eines geeigneten $\wp\xi_0$ entfernt werden. Die Glieder mit $\nu \not\equiv 0$ mod. p lassen sich ferner in die Form

$$\frac{a_\nu}{\pi^\nu} = \left(\frac{a_\nu^{p-1}}{\pi^\kappa}\right)^p \pi^\lambda \quad (1 \leqq \lambda \leqq p-1)$$

setzen, wobei $\nu = \kappa p - \lambda$ gesetzt ist, können also durch Hinzufügen geeigneter $\xi_\lambda^p \pi^\lambda$ entfernt werden. Danach wird auf Grund von Hilfssatz 3

$$(\alpha, \pi) = (a_0, \pi)\,,$$

wo a_0 das konstante Glied in α ist. Dies ist aber gerade durch

$$a_0 = \rho\left(\alpha \frac{d\pi}{\pi}\right)$$

gegeben.

2.) Wir wenden jetzt einen Automorphismus $\pi \to \pi^\sigma = \varepsilon\pi$ (ε beliebige Einheit aus k) von k an, und zwar auf die bereits bewiesene Formel

$$(\alpha, \pi) = (\,\rho\left(\alpha \frac{d\pi}{\pi}\right),\, \pi)\,.$$

VII, 103

Wir erhalten:

$$(\alpha^\sigma, \pi^\sigma) = (\,\rho\left(\alpha \frac{d\pi}{\pi}\right),\, \pi^\sigma)$$

oder nach Hilfssatz 5:

$$(\alpha^\sigma, \pi^\sigma) = (\,\rho\left(\alpha^\sigma \frac{d\pi^\sigma}{\pi^\sigma}\right), \pi^\sigma).$$

Nach Hilfssatz 4 ist aber

$$(r, \pi^\sigma) = (r, \pi\varepsilon) = (r, \pi)\,,$$

wo zur Abkürzung

$$r = \rho\left(\alpha \frac{d\pi}{\pi}\right) = \rho\left(\alpha^\sigma \frac{d\pi^\sigma}{\pi^\sigma}\right)$$

gesetzt ist. Nach Hilfssatz 1 ist somit auch

$$\begin{aligned}(\alpha^\sigma, \pi^\sigma) = (\alpha, \pi) \quad &= \quad (\,\rho\left(\alpha \frac{d\pi}{\pi}\right),\, \pi)\\ &= \quad (\,\rho\left(\alpha^\sigma \frac{d\pi^\sigma}{\pi^\sigma}\right),\, \pi)\end{aligned}$$

oder also indem α^σ wieder durch α ersetzt wird:

$$(\alpha, \varepsilon\pi) = (\,\rho\left(\alpha \frac{d(\varepsilon\cdot\pi)}{\varepsilon\pi}\right),\, \pi)\,.$$

Dann ist die Behauptung für $\beta = \varepsilon\pi$ bewiesen.

3.) Aus

$$(\alpha, \pi) = (\,\rho\left(\alpha\frac{d\pi}{\pi}\right),\,\pi)$$

folgt elementar

$$(\alpha, \pi^{\nu-1}) = (\rho\left(\alpha\frac{d\pi^{\nu-1}}{\pi^{\nu-1}}\right),\,\pi) \quad \text{für alle ganzen} \;\; \nu\,.$$

Multiplikation mit dem in 2.) erhaltenen Resultat liefert

$$(\alpha, \varepsilon\pi^{\nu}) = (\,\rho\left(\alpha\frac{d(\varepsilon\pi^{\nu})}{\varepsilon\pi^{\nu}}\right),\,\pi)\,.$$

Damit ist die Behauptung für jedes beliebige $\beta = \varepsilon\pi^{\nu}$ aus k bewiesen.

7.25 Beweis eines Satzes von Albert über zyklische Algebren. (Feb. 1935)

A central division algebra of prime index p is cyclic if it contains a splitting field of degree p which is pure, i.e., generated by a p-th radical. It appears that Witt had talked in Hasse's seminar about it and produced a particularly simple proof. Hasse was very interested in it since, if this would be true without the assumption that the index is prime then it would be possible to avoid the theorem of Grunwald in the proof of the Brauer-Hasse-Noether theorem on the cyclicity of simple algebras over number fields. However Albert was able to produce a counterexample in 1936 [Alb38]. *See* [Roq05].

VII, 104

Nach E. Witt, Februar 1935

Satz. *Sei k ein Körper mit Char. $\neq p$, D eine normale Divisionsalgebra vom Grade p über k mit einem reinen Zerfällungskörper $k(\sqrt[p]{a})$. Dann ist D zyklisch.*

Beweis. Sei K der Körper der p–ten E. W. über k, $n|p-1$ sein Grad. Dann wird D durch K nicht reduziert, D_K ist also normale Divisionsalgebra vom Grade p über K.

$K(\sqrt[p]{a})$ ist zyklisch über K und Zerfällungskörper für D_K. Dementsprechend besitzt D_K eine Erzeugung:

$$D_K = K(u, v) = (a, \beta, \xi)$$

mit

$$u^p = a, \quad v^p = \beta \quad vu = \zeta\, uv\,,$$

wo $\beta \neq 0$ in K und ζ eine primitive p–te E. W. Sei $\sigma = (\zeta \to \zeta^s)$ ein erz. Autom. für K/k. Da D_K durch Erweiterung von D entsteht, bleibt D_K ungeändert, wenn auf die Erweiterungserzeugung σ angewandt wird. Nach Hilfssatz 1 der vorhergehenden Eintragung] gilt dies dann auch für die obige Erzeugung von D_K:

$$D_K = (a, \beta^\sigma, \zeta^s)\,.$$

VII, 105

Man hat also

$$(a, \beta^\sigma, \zeta^s) = (a, \beta, \zeta)\,.$$

Andererseits gilt bekanntlich

$$(a,\beta^s,\zeta^s)=(a,\beta,\zeta).$$

Somit

$$(a,\beta^\sigma,\zeta^s)=(a,\beta^s,\zeta^s)\,,$$

oder daraus durch Potenzierung mit s

$$(a,\beta^\sigma,\zeta)=(a,\beta^s,\zeta)\,.$$

Daraus folgt leicht:

$$(a,\beta^{\mathsf{S}},\zeta)\sim K$$

für jedes Element $\mathsf{S}\equiv 0$ mod. $(\sigma - s)$ des Gruppenrings von $\{\sigma\}$ über dem Primkörper mod. p.

Wir betrachten speziell das Element

$$C=\frac{1}{n}\sum_\nu s^\nu\sigma^{-\nu}\equiv 1 \mod (\sigma-s)$$

dieses Gruppenrings. Für es folgt:

$$(a,\beta^C,\zeta)=(a,\beta,\zeta)=D_K\,.$$

Daher ist $\gamma=\beta^C\neq 1$ in K. Für dies γ gilt ferner nach Konstruktion

$$\gamma^\sigma=\beta^{C\sigma}\underset{p}{=}\beta^{Cs}=\gamma^s \quad \text{in} \quad K$$

Daher ist bekanntlich $K(\sqrt[p]{\gamma})$ abelsch über k, und daher komponiert aus K mit einem zyklischen Körper Z vom Grade p über k:

$$K(\sqrt[p]{\gamma})=ZK\,.$$

Da

$$D_K=(a,\gamma,\zeta)$$

VII, 106 den Körper $K(\sqrt[p]{\gamma})$ zum Zerfällungskörper hat, wird D durch KZ zerfällt, somit auch durch Z allein, da ${}^{KZ}\!/_{Z}$ vom Grade n ist und daher D_Z nicht zerfällen kann.

D hat also einen zykl. Zerfällungskörper Z vom Grade p über k und ist somit zyklisch.

7.26 Bemerkungen Artins zur A. Weilschen Theorie. (Feb. 1934)

Remark: *We observe that Hasse dates this and the following 5 entries as of February 1934. From February 5 to February 9, 1934 Hasse visited Hamburg and delivered a series of 3 lectures about his new proof of the Riemann hypothesis for elliptic function fields over finite base fields. He had been invited for this by Artin. It appears that these last entries are the result of the discussions which Hasse had during that visit. He may have failed to write down these notes immediately after his return. This would explain that they appear in his notebook after the entries of 1935.*

The present entry contains some comments by Artin on the notion of "distribution" in Weil's thesis where it was proved what today is called the Mordell-Weil theorem [Wei29].

VII, 107

(Februar 1934)

Sei $K = k(x, y)$ ein algebraischer Funktionenkörper über einem algebraischen Zahlkörper k als Konstantenkörper. Sei jedem bzgl. k konjugierten Punktsystem P ein Ideal $\mathfrak{a}(\mathsf{P})$ aus dem zu P gehörigen Restklassenkörper k_{P} (Erweiterung von k) zugeordnet.

Definition. $\mathfrak{a}(\mathsf{P}) \sim 1$, wenn Zähler und Nenner für alle P ein festes Ideal teilen.

Satz. Ist $z(\mathsf{P})$ die einer Funktion des Körpers K entsprechende Idealfunktion (Werte von z an den Stellen P als Hauptideale), so ist $z(\mathsf{P}) \sim 1$.

Weiterer Satz. Ist K'/K unverzweigt, so ist das Ideal der Relativdiskriminante $\mathfrak{d}_{\mathsf{P}} \sim 1$.

Der erste Satz läßt sich auch so aussprechen: Man betrachte die Divisorenklassen der Ordnung 0 von K. Dann existiert eine endliche multiplikative Basis. Durch Übergang zu Idealklassen (Auszeichnung eines Integritätsbereiches) kommt man zu Aussagen über rationale Punkte.

7.27 Konstruktion von Körpern mit beliebig hohem Klassenkörperturm. (Feb. 1934)

Scholz [Sch29] *had shown that the length of class field towers are not bounded. Here Hasse sketches Artin's simple proof (unpublished) where, however, the base field cannot be controlled and may be large. After many years it was shown in 1964 by Golod and Shafarevich that indeed there exist infinite class field towers* [GS64].

VII, 108

(Artin, Februar 1934)

Zu jeder gegebenen endlichen Gruppe $\mathfrak{G}$ kann man einen algebraischen Zahlkörper k mit einem galoisschen Relativkörper K/k der Gruppe $\mathfrak{G}$ konstruieren. Seien $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die Diskriminantenteiler von K/k. Dann sind die zugehörigen Körper $K_{\mathfrak{P}_i}/k_{\mathfrak{p}_i}$ metazyklisch. Man kann nun einen zu K/k fremden Körper $\overline{k}$ so konstruieren, daß er für die Stellen $\mathfrak{p}_i$ mit den $K_{\mathfrak{P}_i}$ übereinstimmt. Dann ist $K\overline{k}/\overline{k}$ unverzweigt mit der Gruppe $\mathfrak{G}$.

So kann man Körper von beliebig hohem Klassenkörperturm konstruieren.

7.28 Über die Funktionalgleichung der Zetafunktion. (Feb. 1934)

On the functional equation of the zeta function according to Artin. The functional equation of the Hecke ϑ-functions (for number fields) is interpreted as an analogon to the Riemann-Roch theorem (for global fields of characteristic p). It appears that already in 1934 Artin harbored ideas which later were formulated more precisely in the thesis of Tate, and that Hasse was quite interested in this. See also 7.19.]

VII, 109

(Artin, Februar 1934)

Sei k ein algebraischer Zahlkörper, $\mathfrak{p}$ eine Primstelle von k, $\alpha \neq 0$ aus k und $\nu_\mathfrak{p}(\alpha)$ die gewöhnliche Ordnungszahl (falls $\mathfrak{p}$ endlich), dagegen $-\log|\alpha|_\mathfrak{p}$ (falls $\mathfrak{p}$ unendlich). Wir ordnen α formal den Divisor

$$\alpha \cong \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\alpha)}$$

zu. Dabei gilt:

1.) Endlichkeit: fast alle $\nu_\mathfrak{p}(\alpha) = 0$

2.) Summenrelation: $\sum_\mathfrak{p} g_\mathfrak{p}\nu_\mathfrak{p}(\alpha) = 0$,
$$\text{wo } g_\mathfrak{p} = \begin{cases} \log \mathfrak{N}(\mathfrak{p}) & (\mathfrak{p} \text{ endlich}) \\ e_\mathfrak{p} = 1 \text{ oder } 2 & (\mathfrak{p} \text{ unendlich}) \end{cases}$$

Beliebige Divisoren seien:

$$\mathfrak{A} = \prod_{\mathfrak{p}\text{ endl.}} \mathfrak{p}^{\nu_\mathfrak{p}} \prod_{\mathfrak{p}\text{ unendl.}} \mathfrak{p}^{-\log\tau_\mathfrak{p}} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}},$$

mit $\nu_\mathfrak{p}$ ganzz. (falls $\mathfrak{p}$ endl.), $\nu_\mathfrak{p} = -\log\tau_\mathfrak{p}$ bel. reell (falls $\mathfrak{p}$ unendl.).

Ganze Divisoren gibt es außer dem Einheitsdivisor definitorisch nicht. Ganz im Endlichen bedeute, daß die endl. $\nu_\mathfrak{p} \geqq 0$ sind. Für das Unendliche wird

$$\mu_\infty(\mathfrak{A}) = \sum_{\mathfrak{p}\text{ unendl.}} e^{-c_\mathfrak{p}\tau_\mathfrak{p}^2} \qquad (c_\mathfrak{p} \text{ geeign. pos. reell})$$

als Maß der Ganzheit eingeführt (Gaußsches Fehlergesetz!). Es ist gleich dem Höchstwert 1 nur für den Einheitsdivisor.

Als Maß der Ganzheit einer Divisorenklasse C wird die Summe der $\mu_\infty(\mathfrak{A})$ für alle im Endlichen ganzen Divisoren der Klasse bezeichnet. Ist also $\mathfrak{a}$ das $\mathfrak{A}$ zugeordnete Ideal (endl. Bestandteil), so ist das Ganzheitsmaß der Klasse C von $\mathfrak{R}$

$$\mu_\infty(C) = \sum_{\alpha \text{ in } \mathfrak{a}^{-1}} e^{-\sum\limits_{\mathfrak{p} \text{ unendl.}} c_\mathfrak{p} \tau_\mathfrak{p}^2 \log|\alpha|_\mathfrak{p}} .$$

VII, 110 Dies ist bei richtiger Normierung der $\tau_\mathfrak{p}$ die Heckesche Thetafunktion. Die Beziehung zwischen den Maßen zweier komplementärer Klassen gibt die Funktionalgleichung der Thetafunktion (Analogon zum Riemann–Rochschen Satz). Als Zetafunktion nehme man nun:

$$\zeta(s) = \int_0^\infty \sum_{\mathfrak{A}} \frac{\mu_\infty(\mathfrak{A})}{\mathfrak{N}(\mathfrak{A})^s} \, d\tau$$

(noch mit einem geeigneten Faktor bei $\mu_\infty(\mathfrak{A})$), über alle im Endlichen ganzen Divisoren $\mathfrak{A}$ summiert und nach den τ integriert. Das gibt dann aus der Funktionalgleichung der Thetafunktion die der Zetafunktion in einfacher Gestalt.

Bei der Reduktion auf die gewöhnliche Zetafunktion stellen sich dann die Γ–Faktoren ein. Bei dieser Reduktion gehe man auf die Primärkomponenten und die ihnen entsprechende Produktzerlegung aus.

7.29 Zwei Bemerkungen zur galoisschen Theorie. (Feb. 1934)

This entry comes from a discussion with Max Zorn. Let $K|k$ be a finite algebraic field extension. If there are only finitely many subextensions then there exists a primitive element for $K|k$. Conversely: If there exists a primitive element then there are only finitely many subextensions.

VII, 111

(Zorn, Februar 1934)

1.) *Aus der Endlichkeit der Zwischenkörperanzahl folgt die Existenz des primitiven Elements (bei unendlichem Grundkörper).*

Seien α, β zwei Elemente aus K und habe K/k nur endlich viele Zwischenkörper. Dann erzeugen mindestens zwei Elemente $\gamma = \alpha + \beta t$ und $\gamma' = \alpha + \beta t'$ ($t \neq t'$ aus k) denselben Zwischenkörper K_0. Dann ist

$$\frac{t'\gamma - t\gamma'}{t' - t} = \alpha\,, \qquad \frac{\gamma - \gamma'}{t - t'} = \beta\,,$$

es liegen also α und β in $K_0 = k(\gamma) = k(\gamma')$, d. h. es ist

$$k(\alpha, \beta) = k(\gamma)\,.$$

Ist also K/k endlich, so ist K/k einfach.

2.) *Aus der Existenz des primitiven Elements folgt die Endlichkeit der Zwischenkörperanzahl.*

Sei ϑ primitives Element für K/k und K_0 ein Zwischenkörper, $\varphi(x)$ das zu ϑ in K_0 gehörige irreduzible Polynom, $K_0' = k(\varphi)$ der Körper der Koeffizienten von φ. Dann ist $K_0' \leqq K_0$ und $[K : K_0] = [K : K_0']$, da φ auch in K_0' irreduzibel ist, also $K_0' = K_0$. Damit ist K_0 auf ein endliches Körpersystem beschränkt, da das irreduzible $f(x)$ in k zu ϑ nur endlich viele Teiler $\varphi(x)$ hat.

7.30 Existenz einer Normalbasis. (Feb. 1934)

The existence of a normal basis has already been the topic of the entry 7.9 of April 1932.] At that time, Hasse recorded a proof by Deuring which worked in any case, regardless of whether the base field is finite or infinite. This time Hasse notes a very simple proof by Artin which, however, works for infinte base fields only. For finite base fields Hasse refers to an old paper by Hensel of the year 1888 [Hen88].

VII, 112

(Artin, Februar 1934)

${}^{K}\!/_{k}$ sei galoissch separabel, k unendlich, $f(x)$ ein erzeugendes Polynom, α eine seiner Wurzeln, und S durchlaufe die Gruppe von ${}^{K}\!/_{k}$. Sei

$$\varphi(x) = \frac{f(x)}{(x-\alpha)f'(\alpha)}\,,$$

dann gilt

$$\varphi(x)^{\mathsf{S}} \equiv 1 \;\text{mod.}\; x-\alpha^{\mathsf{S}}, \quad \equiv 0 \;\text{mod.}\; x-\alpha^{\mathsf{S}'} \quad (\mathsf{S}' \neq \mathsf{S})$$

also

$$\left|\varphi(x)^{\mathsf{ST}^{-1}}\right|^2 \equiv 1 \;\text{mod.}\; f(x)\,.$$

Folglich ist x in k so spezialisierbar, daß

$$\left|\varphi(x)^{\mathsf{ST}^{-1}}\right| \neq 0$$

ist. Dann bilden die $\varphi(x)^{\mathsf{S}}$ eine Normalbasis.

Teil III

Verzeichnisse

Kapitel 8

Namenverzeichnis

Kapitel 9

Bibliographie

[AH25] E. Artin and H. Hasse. Über den zweiten Ergänzungssatz zum Reziprozitätsgesetz der l–ten Potenzreste im Körper k_ζ der l-ten Einheitswurzeln und in Oberkörpern von k_ζ. *J. Reine Angew. Math.*, 154:143–148, 1925.

[AH28] E. Artin and H. Hasse. Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n-ten Potenzreste im Körper der l^n-ten Einheitswurzeln. *Abh. Math. Semin. Univ. Hamb.*, 6:146–162, 1928.

[Alb38] A.A. Albert. Non-cyclic algebras with pure maximal subfields. *Bull. Amer. Math. Soc.*, 44:576–579, 1938.

[Art23] E. Artin. Über die Zetafunktionen gewisser algebraischer Zahlkörper. *Math. Ann.*, 89:147–156, 1923.

[Art27] E. Artin. Beweis des allgemeinen Reziprozitätsgesetzes. *Abh. Math. Semin. Univ. Hamb.*, 5:353–363, 1927.

[Art31] E. Artin. *Einführung in die Theorie der Gammafunktion.*, volume 11 of *Hamburger Mathematische Einzelschriften.* B. G. Teubner, Leipzig, 1931. 35 pp.

[Art57] E. Artin. *Geometric algebra.* Interscience tracts in pure and applied mathematics. Interscience Publ., 1957. X+214 pp.

[BH65] L. Bernstein and H. Hasse. Einheitenberechnung mittels des Jacobi-Perronschen Algorithmus. *J. Reine Angew. Math.*, 218:51–69, 1965.

[BH69] L. Bernstein and H. Hasse. Explicit determination of the Perron matrices in periodic algorithms of the Perron-Jacobi type with application to generalized Fibonacci numbers with time impulses. *Fibonacci Q.*, 7:394–436, 1969.

[Bôc07] M. Bôcher. *Introduction to higher akgebra. Prepared for publication with the cooperation of E. P. R. Duval.* The Macmillan Co., London, 1907. 321 pp.

[Bre24] S. Breuer. Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad.). *Math. Ann.*, 92:126–144, 1924.

[Che33a] C. Chevalley. La théorie du symbole de restes normiques. *J. Reine Angew. Math.*, 169:140–157, 1933.

[Che33b] C. Chevalley. Sur la théorie du corps de classes dans les corps finis et les corps locaux. *J. Fac. Sci. Univ. Tokyo*, Sect. I 2:365–476, 1933.

[Che34] C. Chevalley. Sur certains idéaux d'une algèbre simple. *Abh. Math. Semin. Univ. Hamb.*, 10:83–105, 1934.

[Chi51] A.J. Chintschin. *Three pearls of number theory. Translated from the Russian. (Drei Perlen der Zahlentheorie.).* Akademie-Verlag, Berlin, 1951. 62 pp.

[Coh78] H. Cohn. *A classical invitation to algebraic numbers and class fields. With two appendices by Olga Taussky: "Artin's 1932 Göttingen lectures on class field theory" and "Connections between algebraic number theory and integral matrices.".* Universitext. Springer–Verlag, New York – Heidelberg – Berlin, 1978. XIII, 328 pp.

[Cur22] D. R. Curtiss. On Kellogg's diophantine problem. *American Math. Monthly*, 29:380–387, 1922.

[Dav33] H. Davenport. On certain exponential sums. *J. Reine Angew. Math.*, 169:158–176, 1933.

[Deu32] M. Deuring. Galoissche Theorie und Darstellungstheorie. *Math. Ann.*, 107:140–144, 1932.

[Dir28] L. Dirichlet. Mémoire sur lŠimpossibilité de quelques quations indéterminé du cinquième degré. *J. Reine Angew. Math.*, 3:354–375, 1828.

[Dör25] K. Dörge. Zum Hilbertschen Irreduzibilitätssatz. *Math. Ann.*, 95:84–97, 1925.

[Dör26a] K. Dörge. Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. *Math. Ann.*, 96:176–182, 1926.

[Dör26b] K. Dörge. Zum Hilbertschen Irreduzibilitätssatz. *Jber. Deutsch. Math. Verein.*, 34:145, 1926.

[EH67] L. Elsner and H. Hasse. Numerische Ergebnisse zum Jacobischen Kettenbruchalgorithmus in rein-kubischen Zahlkörpern. *Math. Nachr.*, 34:95–97, 1967.

[Eis44] G. Eisenstein. Entwicklung von $\alpha^{\alpha^{\cdot^{\cdot^{\cdot}}}}$. *J. Reine Angew. Math.*, 28:49–52, 1844.

[Eis50] G. Eisenstein. Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. *J. Reine Angew. Math.*, 39:351–364, 1850. Nachdruck in Mathematische Werke, Band II, [36], pp. 623–636.

[Els98] J. Elstrodt. Partialbruchentwicklung des Kotangens, Herglotz-Trick und die Weierstraßche stetige, nirgends differenzierbare Funktion. *Math. Semesterber.*, 45:207–220, 1998.

[FR08] G. Frei and P. Roquette, editors. *Emil Artin and Helmut Hasse. Their correspondence 1923-1934. With contributions of Franz Lemmermeyer and an introduction in English.* Universitäts–Verlag, Göttingen, 2008. 497 pp.

[Fra31] W. Franz. Untersuchungen zum Hilbertschen Irreduzibilitätssatz. *Math. Zeitschr.*, 33:275–293, 1931.

[Fro03] G. Frobenius. Theorie der hyperkomplexen Größen i. ii. *Sitzungsberichte Akad. Berlin*, 1903:504–537, 634–645, 1903.

[Fro14a] G. Frobenius. Über das quadratische Reziprozitätsgesetz i. *Sitzungsberichte Akad. Berlin*, 1914:335–349, 1914. Ges. Abhandl.. 628–642.

[Fro14b] G. Frobenius. Über das quadratische Reziprozitätsgesetz ii. *Sitzungsberichte Akad. Berlin*, 1914:484–488, 1914. Ges. Abhandl., 643–647.

[Fur08] Ph. Furtwängler. Über die Klassenzahlen Abelscher Zahlkörper. *J. Reine Angew. Math.*, 134:91–94, 1908.

[Fur12] Ph. Furtwängler. Letzter Fermatscher Satz und Eisensteinsches Reziprozitätsprinzip. *Sitz.-Ber. Akad. Wiss. Wien*, 121:589–592, 1912.

[Fur16] Ph. Furtwängler. Über das Verhalten der Ideale des Grundkörpers im Klassenkörper. *Monatshefte f. Math. u. Phys.*, 27:1–15, 1916.

[Gre27] H. Grell. Zur Theorie der Ordnungen in algebraischen Zahl- und Funktionenkörpern. *Math. Ann.*, 97:524–558, 1927.

[GS64] E. Golod and I. Shafarevich. On class field towers. *Am. Math. Soc. Translations (2).*, 48:91–102, 1964.

[Hac11] F. Hack. *Wahrscheinlichkeitsrechnung.* Göschen, Leipzig, 1911. 122 pp.

[Has24a] H. Hasse. Das allgemeine Reziprozitätsgesetz und seine Ergänzungssätze in beliebigen algebraischen Zahlkörpern für gewisse, nichtprimäre Zahlen. *J. Reine Angew. Math.*, 153:192–207, 1924.

[Has24b] H. Hasse. Zur Theorie des Hilbertschen Normenrestsymbols in algebraischen Zahlkörpern. Zweiter Teil: Fall eines ungeraden ℓ. *J. Reine Angew. Math.*, 153:184–191, 1924.

[Has25a] H. Hasse. Das allgemeine Reziprozitätsgesetz der l-ten Potenzreste für beliebige, zu l prime Zahlen in gewissen Oberkörpern des Körpers der l-ten Einheitswurzeln. *J. Reine Angew. Math.*, 154:199–214, 1925.

[Has25b] H. Hasse. Der zweite Ergänzungssatz zum Reziprozitätsgesetz der l-ten Potenzreste für beliebige, zu l prime Zahlen in gewissen Oberkörpern des Körpers der l-ten Einheitswurzeln. *J. Reine Angew. Math.*, 154:215–218, 1925.

[Has25c] H. Hasse. Über das allgemeine Reziprozitätsgesetz der l-ten Potenzreste im Körper k_ζ der l-ten Einheitswurzeln und in Oberkörpern von k_ζ. *J. Reine Angew. Math.*, 154:96–109, 1925.

[Has25d] H. Hasse. Zur Theorie des Hilbertschen Normenrestsymbols in algebraischen Zahlkörpern. Dritter Teil: Normierung. *J. Reine Angew. Math.*, 154:174–177, 1925.

[Has26a] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. I: Klassenkörpertheorie. *Jahresber. Dtsch. Math.-Ver.*, 35:1–55, 1926.

[Has26b] H. Hasse. Neue Begründung der komplexen Multiplikation. I. Einordnung in die allgemeine Klassenkörpertheorie. *J. Reine Angew. Math.*, 157:115–139, 1926.

[Has27a] H. Hasse. Das Eisensteinsche Reziprozitätsgesetz der n-ten Potenzreste. *Math. Ann.*, 97:599–623, 1927.

[Has27b] H. Hasse. Über das Reziprozitätsgesetz der m-ten Potenzreste. *J. Reine Angew. Math.*, 158:228–259, 1927.

[Has29] H. Hasse. Zum expliziten Reziprozitätsgesetz. *Abh. Math. Semin. Univ. Hamb.*, 7:52–63, 1929.

[Has30a] H. Hasse. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Zeitschr.*, 31:565–582, 1930.

[Has30b] H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. II: Reziprozitätsgesetz. *Jahresber. Dtsch. Math.-Ver.*, 6(Ergänzungsband), 1930. IV + 204 pp.

[Has30c] H. Hasse. Die Normenresttheorie relativ–Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen. *J. Reine Angew. Math.*, 162:145–154, 1930.

[Has31] H. Hasse. Neue Begründung der komplexen Multiplikation. II. Aufbau ohne Benutzung der allgemeinen Klassenkörpertheorie. *J. Reine Angew. Math.*, 165:64–88, 1931.

[Has32] H. Hasse. Zwei Bemerkungen zu der Arbeit "Zur Arithmetik der Polynome" von U. Wegner. *Math. Ann.*, 106:455–456, 1932.

[Has33a] H. Hasse. Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. Insbesondere Begründung der Theorie des Normenrestsymbols und Herleitung des Reziprozitätsgesetzes mit nichtkommutativen Hilfsmitteln. *Math. Ann.*, 107:731–760, 1933.

[Has33b] H. Hasse. Vorlesungen über Klassenkörpertheorie. Preprint, Marburg. [Later published in book form by Physica Verlag Würzburg (1967)], 1933.

[Has34] H. Hasse. Über gewisse Ideale in einer einfachen Algebra. (Exposés mathématiques, publiés à la mémoire de Jacques Herbrand, I.). *Actual. Sci. Ind.*, 1934(109):12–16, 1934.

[Has49] H. Hasse. Invariante Kennzeichnung relativ-abelscher Zahlörper mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers. *Abh. Deutsch. Akad. Wiss. Berlin Kl. Math. Nat. Wiss.*, 1947(8):56 pp., 1949.

[Has52] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper.* Akademie–Verlag, Berlin, 1952. Reprint 1985 with an introduction of J. Martinet.

[Has58] H. Hasse. Der 2^n-te Potenzcharakter von 2 im Körper der 2^n-ten Einheitswurzeln. *Rend. Circ. Mat. Palermo, II. Ser.*, 7:185–244, 1958.

[Hen88] K. Hensel. Über die Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor. *J. Reine Angew. Math.*, 53:230–237, 1888.

[Hen16] K. Hensel. Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers. *J. Reine Angew. Math.*, 146:189–215, 1916.

[Hes04] G. Hessenberg. Über einen geometrischen Kalkul (Verknüpfungs-Kalkul). *Acta Math.*, 29:1–24, 1904.

[Hil99] D. Hilbert. *Grundlagen der Geometrie. (Festschrift zur Feier der Enthüllung des Gauss-Weber-Denkmals in Göttingen.).* B. G. Teubner., Leipzig, 1899. 92 pp.

[Hil98] D. Hilbert. *The theory of algebraic number fields. Transl. from the German by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher.* Springer, Berlin, 1998. xxxvi, 350 pp.

[Hon76] K. Honda. Teiji Takagi: A biography. On the 100th anniversary of his birth. *Comment. Math. Univ. St. Pauli*, 24:141–167, 1976.

[HS31] H. Hasse and Z. Suetuna. Ein allgemeines Teilerproblem der Idealtheorie. *J. Fac. Sci. Univ. Tokyo*, Section I, vol.II, Part 5:133–154, 1931.

[HT28] H. Hasse and E. Tornier. Über die Dichte der quadratfreien Zahlen und ähnliche Dichten in einem algebraischen Zahlkörper. *Berichte d. Akad. d. Naturforscher zu Halle*, 3:9–16, 1928.

[Jac07] Jacobsthal. Über die Darstellung der Primzahlen der Form 4n+1 als Summe zweier Quadrate. *J. Reine Angew. Math.*, 132:238–246, 1907.

[Kel21] O. D. Kellogg. On a diophantine problem. *Amer. Math. Monthly*, 28:300–303, 1921.

[Lem00] F. Lemmermeyer. *Reciprocity Laws. From Euler to Eisenstein.* Springer–Verlag, Berlin, Heidelberg, New York, 2000. XIX, 487 pp.

[LR06] F. Lemmermeyer and P. Roquette, editors. *Helmut Hasse and Emmy Noether. Their correspondence 1925-1935. With an introduction in English.* Universitäts–Verlag, Göttingen, 2006. 303 pp.

[Met07] T. Metsänkylä. On the history of the study of ideal class groups. *Expositiones Math.*, 25:325–340, 2007.

[Mor33] L. J. Mordell. The number of solutions of some congruences in two variables. *Math. Zeitschr.*, 37:193–209, 1933.

[Noe17] E. Noether. Gleichungen mit vorgeschriebener Gruppe. *Math. Ann.*, 78:221–229, 1917.

[Noe34] E. Noether. Zerfallende verschränkte Produkte und ihre Maximalordnungen. (Exposés mathématiques, publiés à la mémoire de Jacques Herbrand, IV.). *Actual. Sci. Ind.*, 1934(148):15 p., 1934.

[Per07] O. Perron. Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus. *Math. Ann.*, 64:1–76, 1907.

[Rei33] H. Reichardt. Arithmetische Theorie der kubischen Körper als Radikalkörper. *Monatsh. Math. Phys.*, 40:323–350, 1933.

[Roq04] P. Roquette. The Riemann hypothesis in characteristic p, its origin and development. Part 2. The first steps by Davenport and Hasse. *Mitt. Math. Ges. Hamburg*, 22:1–69, 2004.

[Roq05] P. Roquette. *The Brauer-Hasse-Noether Theorem in historical perspective.*, volume 15 of *Schriftenreihe der Heidelberger Akademie der Wissenschaften*. Springer–Verlag, Berlin, Heidelberg, New York, 2005. I, 77 pp.

[Roq12] P. Roquette. The Riemann hypothesis in characteristic p, its origin and development. Part 4. Davenport-Hasse fields. *Mitt. Math. Ges. Hamburg*, 30:193–204, 2012.

[Sch29] A. Scholz. Zwei Bemerkungen zum Klassenkörperturm. *J. Reine Angew. Math.*, 161:201–207, 1929.

[Sch35] H. L. Schmid. Über das Reziprozitätsgesetz in relativ–zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper. *Math. Z.*, 40:91–109, 1935.

[Sch94] G. Schuppener. *Geschichte der Zeta-Funktion von Oresme bis Poisson.* Deutsche Hochschulschriften. Hänsel-Hohenhausen, Egelsbach, 1994. 196 pp.

[Ste03] P. Stevenhagen. The correction factor in Artin's primitive root conjecture. *J. Théor. Nombres Bordeaux.*, 15(1):283–391, 2003.

[Swa69] R. G. Swan. Invariant rational functions and a problem of Steenrod. *Invent. Math*, 7:148–158, 1969.

[Tak20] T. Takagi. Über eine Theorie des relativ abelschen Zahlkörpers. *J. College of Science, Imp. Univ. of Tokyo.*, 41:1–133, 1920. In Collected Papers, 13., pp. 73–167.

[Tak22] T. Takagi. Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper. *J. College of Science, Imp. Univ. of Tokyo.*, 44:1–50, 1922. In Collected Papers, 17., pp. 179–216.

[Tsc24] N. Tschebotareff. Eine Verallgemeinerung des Minkowskischen Satzes mit Anwendung auf die Betrachtung der Körperidealklassen. *Ber. wiss. Forsch. Inst. Odessa*, 1(4):17–20, 1924.

[Tsc29] N. Tschebotareff. Zur Gruppentheorie des Klassenkörpers. *J. Reine Angew. Math.*, 161:179–193, 1929.

[vdW27] B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Archief*, 15:212–216, 1927.

[vdW34] B. L. van der Waerden. Elementarer Beweis eines zahlentheoretischen Existenztheorems. *J. Reine Angew. Math.*, 171:1–3, 1934.

[vdW98] B. L. van der Waerden. How the proof of baudetŠs conjecture was found. (wie der beweis der vermutung von baudet gefunden wurde.). *Elem. Math.*, 1998(53):139–148, 1998.

[Ven32] H. Vennekohl. Neuer Beweis für die explizite Reziprozitätsformel der ℓ-ten Potenzreste im ℓ-ten Kreiskörper. *Math. Ann.*, 107:233–251, 1932.

[Was82] L. Washington. *Introduction to Cyclotomic Fields.* Spinger, Berlin, 2 edition, 1982. 487 pp.

[Wei29] A. Weil. L'arithmétique sur les courbes algébriques. *Acta Math.*, 52:281–315, 1929.

[Wie09] A. Wieferich. Zum letzten Fermatschen Theorem. *J. Reine Angew. Math.*, 136:293–302, 1909.

[Wit35a] E. Witt. Der Existenzsatz für abelsche Funktionenkörper. *J. Reine Angew. Math.*, 173:43–51, 1935.

[Wit35b] E. Witt. Zwei Regeln über verschränkte Produkte. *J. Reine Angew. Math.*, 173:191–192, 1935.

This book contains the full text of the mathematical notebooks of Helmut Hasse (1898–1979), who was one of the leading mathematicians of the 20th century. The originals have been preserved in the Handschriftenabteilung at the Göttingen University Library. There are a total of seven volumes which contain 98 entries all together; these span the time period from July 1923 to February 1935. Each of the entries is preceded by a short comment. An extensive bibliography is provided.

Compared to the other documents and papers from Hasse Nachlass at Göttingen, these papers are quite different. They detail Hasse's mathematical background, interests and his way of approaching problems. Many of the entries are inspired by Hasse's discussions with other mathematicians (for example, Emil Artin is often mentioned).

One of the notable highlights in the entries is the first documentation of Artin's conjecture on primitive roots (1927), which Hasse noted down after a discussion with Artin. Another example is the first proof of the Riemann hypothesis for an extended class of function fields of high genus, namely those of the generalised Fermat fields with a finite field of constants (1932), after corresponding with Harold Davenport.



ISBN 978-3-86395-072-9

Universitätsverlag Göttingen